SUSE Linux Référence

www.novell.com

10.0 | 13/09/2005



Référence

Auteurs: Jörg Arndt, Stefan Behlert, Frank Bodammer, James Branam, Volker Buzek, Klara Cihlarova, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Thorsten Dubiel, Torsten Duwe, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Joachim Gleißner, Carsten Groß, Andreas Grünbacher, Berthold Gunreben, Franz Hassels, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Edith Parzefall, Peter Pöml, Thomas Renninger, Hannes Reinecke, Thomas Rölz, Heiko Rommel, Marcus Schäfer, Thomas Schraitle, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz

Adressez vos suggestions et commentaire à `documentation@suse.de`.

Table des matières

À propos de ce guide **xv**

Partie I Scénarios de déploiement avancés **19**

1 Installation à distance **21**

1.1 Scénarios d'installation à distance 21
1.2 Configuration du serveur qui contient les sources d'installation 31
1.3 Préparation du démarrage du système cible 41
1.4 Démarrage du système cible pour l'installation 52
1.5 Surveillance du processus d'installation 57

2 Configuration avancée des disques **61**

2.1 Noms de périphérique permanents pour les périphériques SCSI 61
2.2 Configuration du gestionnaire de volumes logiques (LVM) 62
2.3 Configuration de Soft RAID 70

Partie II Internet **77**

3 Le navigateur Web Konqueror **79**

3.1 Navigation par onglets 80
3.2 Enregistrement de pages Web et de graphiques 81
3.3 Mots-clés Internet 81
3.4 Signets 82
3.5 Java et JavaScript 83
3.6 Pour plus d'informations 84

4 Firefox **85**

4.1 Consultation de sites Web 85
4.2 Recherche d'informations 87
4.3 Gestion des marque-pages 87
4.4 Utilisation du gestionnaire de téléchargements 90
4.5 Personnalisation de Firefox 90
4.6 Impression à partir de Firefox 93
4.7 Pour plus d'informations 94

5 Linphone—VoIP pour Linux Desktop **95**

5.1 Configuration de Linphone 95
5.2 Test de Linphone 101
5.3 Appel d'un correspondant 101
5.4 Réponse à un correspondant 103
5.5 Utilisation du carnet d'adresses 103
5.6 Dépannage 104
5.7 Glossaire 105
5.8 Pour plus d'informations 106

6 Le chiffrement avec KGpg **107**

6.1 Génération d'une nouvelle paire de clés 107
6.2 Exportation de la clé publique 109
6.3 Importation de clés 110
6.4 La boîte de dialogue Serveur de clés 111
6.5 Chiffrement de texte et de fichiers 114
6.6 Pour plus d'informations 115

Partie III Multimédia **117**

7 Son dans Linux **119**

7.1 Mixeurs 119
7.2 Lecteurs multimédias 125
7.3 CD : lecture et extraction (RIP) 131
7.4 Enregistrement sur disque dur avec Audacity 136
7.5 Lecture et enregistrement directs de fichiers WAV 139

8 TV, Vidéo, Radio et Webcam **141**

8.1 Regarder la télévision avec motv 141
8.2 Prise en charge du vidéotexte 144
8.3 Webcams et motv 144

8.4 nxtvepg : le magasine télé de votre PC 145
8.5 Regarder des émissions vidéo numériques avec xawtv4 147

9 K3b – Gravure de CD ou de DVD 151

9.1 Création d'un CD de données 151
9.2 Création d'un CD audio 154
9.3 Copie d'un CD ou d'un DVD 155
9.4 Gravure d'images ISO 156
9.5 Création d'un CD ou d'un DVD multisession 157
9.6 Pour plus d'informations 158

Partie IV Bureautique 159

10 Suite bureautique OpenOffice.org 161

10.1 Compatibilité avec d'autres applications de bureautique 162
10.2 Traitement de texte avec OpenOffice.org Texte 164
10.3 Présentation de Calc 167
10.4 Présentation d'Impress 167
10.5 Présentation de Base 168
10.6 Pour plus d'informations 169

11 Evolution : programme de messagerie et de gestion d'agenda 171

11.1 Importation des messages électroniques depuis d'autres programmes de messagerie 171
11.2 Présentation d'Evolution 172
11.3 Messagerie 174
11.4 Contacts 178
11.5 Agendas 180
11.6 Synchronisation des données avec un périphérique de poche 182
11.7 Evolution pour les utilisateurs GroupWise 182
11.8 Pour plus d'informations 183

12 Kontact : programme de messagerie et de gestion d'agenda 185

12.1 Importation des messages électroniques depuis d'autres programmes de messagerie 185
12.2 Présentation de Kontact 186
12.3 Messagerie 188
12.4 Contacts 193
12.5 Calendrier 196
12.6 Synchronisation des données avec un périphérique de poche 198
12.7 Kontact pour les utilisateurs GroupWise 198

12.8 Pour plus d'informations 200

13 Synchronisation d'un périphérique de poche avec KPilot 201

13.1 Conduits utilisés par KPilot 202
13.2 Configuration de la connexion avec le périphérique de poche 203
13.3 Configuration du conduit KAddressBook 204
13.4 Gestion des tâches et des événements 205
13.5 Utilisation de KPilot 206

14 Utilisation de Beagle 209

14.1 Indexation des données 210
14.2 Recherche de données 212

Partie V Applications graphiques 215

15 Appareils photo numériques et Linux 217

15.1 Connexion avec l'appareil photo numérique 217
15.2 Accès à l'appareil photo 218
15.3 Utilisation de Konqueror 219
15.4 Utilisation de Digikam 219
15.5 Utilisation de f-spot 229
15.6 Pour plus d'informations 237

16 Kooka — Application de numérisation 239

16.1 L'aperçu 240
16.2 La numérisation finale 241
16.3 Les menus 242
16.4 La galerie 243
16.5 Reconnaissance optique des caractères 244

17 Manipulation des graphiques au moyen de GIMP 247

17.1 Formats de graphiques 247
17.2 Démarrage de GIMP 248
17.3 Mise en route de GIMP 250
17.4 Enregister des images 252
17.5 Impression des images 253
17.6 Pour plus d'informations 254

Partie VI Mobilité 257

18 Informatique mobile avec Linux 259

18.1 Ordinateurs portables 259
18.2 Matériel mobile 267
18.3 Téléphones cellulaires et assistants personnels 268
18.4 Pour plus d'informations 268

19 PCMCIA 271

19.1 Matériel 271
19.2 Logiciel 272

20 Gestion du profil de configuration du système (SCPM, System Configuration Profile Management) 273

20.1 Terminologie 274
20.2 Utilisation du gestionnaire de profils YaST 274
20.3 Configuration de SCPM via la ligne de commande 278
20.4 Utilisation de l'applet Sélecteur de profil 282
20.5 Dépannage 282
20.6 Sélection d'un profil au démarrage du système 283
20.7 Pour plus d'informations 284

21 Gestion de l'alimentation 285

21.1 Fonctions d'économie d'énergie 286
21.2 APM 287
21.3 ACPI 288
21.4 Repos du disque dur 296
21.5 Paquetage powersave 297
21.6 Module de gestion de l'alimentation YaST 306

22 Communications sans fil 311

22.1 Réseau local sans fil 311
22.2 Bluetooth 322
22.3 Transmission de données infrarouge 334

Partie VII Administration **339**

23 Sécurité sous Linux 341

23.1 Masquage et pare-feux 341
23.2 SSH – travailler en réseau en toute sécurité 352
23.3 Codage des partitions et des fichiers 358
23.4 Sécurité et confidentialité 362

24 Listes de contrôle d'accès sous Linux 377

24.1 Avantages des ACL 377
24.2 Définitions 378
24.3 Gestion des ACL 379
24.4 Prise en charge des ACL dans les applications 387
24.5 Pour plus d'informations 388

25 Utilitaires de surveillance du système 389

25.1 Liste des fichiers ouverts : `lsof` 390
25.2 Utilisateur qui accède aux fichiers : `fuser` 391
25.3 Propriétés d'un fichier : `stat` 391
25.4 Périphériques USB : `lsusb` 392
25.5 Informations relatives à un périphérique SCSI : `scsiinfo` 393
25.6 Processus : `top` 393
25.7 Liste des processus : `ps` 394
25.8 Arborescence de processus : `pstree` 396
25.9 Qui fait quoi : `w` 397
25.10 Utilisation de la mémoire : `free` 397
25.11 Tampon circulaire du kernel : `dmesg` 398
25.12 Les systèmes de fichiers et leur utilisation : `mount`, `df` et `du` 399
25.13 Le système de fichiers `/proc` 400
25.14 Commandes `vmstat`, `iostat` et `mpstat` 402
25.15 `procinfo` 402
25.16 Ressources PCI : `lspci` 403
25.17 Appels système d'une exécution de programme : `strace` 405
25.18 Appels de bibliothèque d'une exécution de programme : `ltrace` . . . 406
25.19 Spécification de la bibliothèque requise : `ldd` 406
25.20 Informations supplémentaires sur les fichiers binaires ELF 407
25.21 Communication entre processus : `ipcs` 408
25.22 Calculs de durée avec `time` 408

Partie VIII Système 409

26 Applications 32 bits et 64 bits dans un environnement système 64 bits 411

26.1 Prise en charge de l'exécution 411
26.2 Développement de logiciels 412
26.3 Compilation de logiciels sur des plates-formes biarch (à double architecture) . 413
26.4 Spécifications du kernel 414

27 Utilisation du shell 417

27.1 Utilisation de Bash sur la ligne de commande 417
27.2 Utilisateurs et autorisations d'accès 429
27.3 Commandes Linux importantes 435
27.4 L'éditeur vi 448

28 Amorçage et configuration d'un système Linux 453

28.1 Le processus d'amorçage de Linux 453
28.2 Le processus init 457
28.3 Configuration système via /etc/sysconfig 466

29 Chargeur d'amorçage 471

29.1 Gestion de l'amorçage 472
29.2 Sélection d'un chargeur d'amorçage 473
29.3 Amorçage à l'aide de GRUB 473
29.4 Configuration du chargeur d'amorçage à l'aide de YaST 484
29.5 Désinstallation du chargeur d'amorçage Linux 490
29.6 Créer des CD d'amorçage 490
29.7 Écran graphique SUSE 491
29.8 Dépannage 492
29.9 Pour plus d'informations 494

30 Caractéristiques spécifiques à SUSE Linux 495

30.1 Informations à propos des paquetages logiciel spéciaux 495
30.2 Consoles virtuelles 502
30.3 Affectation des touches du clavier 503
30.4 Paramètres spécifiques aux langues et aux pays 504

31 Fonctionnement de l'imprimante 509
31.1 Workflow du système d'impression . . . 511
31.2 Méthodes et protocoles de connexion d'imprimantes . . . 511
31.3 Installation du logiciel . . . 512
31.4 Configuration de l'imprimante . . . 513
31.5 Configuration des applications . . . 520
31.6 Particularités de SUSE Linux . . . 521
31.7 Dépannage . . . 527

32 Le système Hotplug 535
32.1 Périphériques et interfaces . . . 536
32.2 Evénements hotplug . . . 537
32.3 Configuration des périphériques hotplug . . . 537
32.4 Chargement automatique des modules . . . 540
32.5 La commande de démarrage coldplug . . . 540
32.6 Analyse des erreurs . . . 540

33 Noeuds de périphériques dynamiques avec udev 543
33.1 Création de règles . . . 544
33.2 Substitution d'espaces réservés . . . 545
33.3 Correspondance de modèle dans les clés . . . 545
33.4 Sélection des clés . . . 545
33.5 Noms persistants pour les périphériques de stockage de masse . . . 547

34 Systèmes de fichiers sous Linux 549
34.1 Terminologie . . . 549
34.2 Les principaux systèmes de fichiers sous Linux . . . 550
34.3 Autres systèmes de fichiers pris en charge . . . 558
34.4 Prise en charge des fichiers volumineux sous Linux . . . 559
34.5 Pour plus d'informations . . . 561

35 Système X Window 563
35.1 Configuration de X11 avec SaX2 . . . 563
35.2 Optimisation de la configuration X . . . 565
35.3 Installation et configuration de polices . . . 571
35.4 Configuration de OpenGL—3D . . . 577

36 Authentification avec les modules PAM 581
36.1 Structure d'un fichier de configuration PAM . . . 582

36.2 Configuration PAM de sshd 584
36.3 Configuration des modules PAM 586
36.4 Pour plus d'informations 588

37 Virtualisation avec Xen 591

37.1 Installation de Xen 593
37.2 Installation de domaines 594
37.3 Configuration d'un domaine invité Xen 598
37.4 Démarrage et contrôle de domaines Xen 599
37.5 Pour plus d'informations 600

Partie IX Services 603

38 Bases de la mise en réseau 605

38.1 Adresses IP et routage 609
38.2 IPv6 : Internet nouvelle génération 612
38.3 Résolution de noms 621
38.4 Configuration d'une connexion réseau avec YaST 623
38.5 Configuration manuelle d'une connexion réseau 635
38.6 smpppd comme assistant de connexion 646

39 Services SLP sur le réseau 651

39.1 Enregistrement de vos propres services 651
39.2 Interfaces client SLP dans SUSE Linux 653
39.3 Activation de SLP 653
39.4 Pour plus d'informations 654

40 La résolution de noms 655

40.1 Notions de base du DNS 655
40.2 Configuration avec YaST 655
40.3 Démarrer le serveur de noms BIND 663
40.4 Le fichier de configuration /etc/named.conf 665
40.5 Fichiers de zone 669
40.6 Actualisation dynamique des données de zones 674
40.7 Transactions sécurisées 674
40.8 Sécurité de DNS 676
40.9 Informations supplémentaires 676

41 Utilisation de NIS **677**

41.1 Configuration des serveurs NIS à l'aide de YaST 677
41.2 Configuration des clients NIS 683

42 Partage des systèmes de fichiers avec NFS **685**

42.1 Importation de systèmes de fichiers avec YaST 685
42.2 Importation manuelle des systèmes de fichiers 686
42.3 Exportation de systèmes de fichiers avec YaST 687
42.4 Exportation manuelle des systèmes de fichiers 688

43 DHCP **691**

43.1 Configuration d'un serveur DHCP avec YaST 692
43.2 Paquetages logiciels DHCP 696
43.3 Le démon dhcpd du serveur DHCP 697
43.4 Pour plus d'informations 701

44 Synchronisation avec xntp **703**

44.1 Configuration d'un client NTP avec YaST 703
44.2 Configuration de xntp dans le réseau 707
44.3 Configuration d'une horloge de référence locale 708

45 LDAP - Service d'annuaire **709**

45.1 LDAP vs NIS 711
45.2 Structure d'une arborescence LDAP 712
45.3 Configuration de serveur avec slapd.conf 715
45.4 Gestion de données dans l'annuaire LDAP 720
45.5 Client LDAP de YaST 724
45.6 Configuration d'utilisateurs et de groupes LDAP dans YaST 732
45.7 Pour plus d'informations 734

46 Le serveur Web Apache **737**

46.1 Préface et terminologie 737
46.2 Installation 739
46.3 Configuration 747
46.4 Hôtes virtuels 763
46.5 Modules Apache 767
46.6 Sécurité 779
46.7 Dépannage 781
46.8 Pour plus d'informations 782

47 Synchronisation des fichiers 785

47.1 Logiciels pour la synchronisation des données 785
47.2 Critères de choix du logiciel 788
47.3 Introduction à Unison 793
47.4 Introduction à CVS 795
47.5 Introduction à Subversion 797
47.6 Introduction à rsync 801
47.7 Introduction à mailsync 803

48 Samba 807

48.1 Configuration du serveur 809
48.2 Samba utilisé comme serveur de login 814
48.3 Configuration d'un serveur Samba avec YaST 815
48.4 Configuration des clients 818
48.5 Optimisation 819

Index 821

À propos de ce guide

Ce manuel vous permet d'avoir une vision globale de SUSE Linux. Il s'adresse principalement aux administrateurs système, ainsi qu'aux particuliers qui disposent de connaissances dans le domaine de l'administration système. Vous trouverez dans ce manuel une sélection d'applications utiles au quotidien, accompagnées d'une description détaillée de scénarios d'installation et de configuration.

Scénarios de déploiement avancés
Apprenez à déployer SUSE Linux dans des environnements complexes.

Internet, multimédia, bureautique et graphisme
Faites un tour d'horizon des applications les plus importantes pour un particulier.

Mobilité
Familiarisez-vous avec l'informatique mobile grâce à SUSE Linux, et apprenez à configurer les différentes options relatives au mode sans fil, à la gestion de l'alimentation et à la gestion des profils.

Administration
Apprenez à sécuriser SUSE Linux et à gérer les contrôles d'accès au système de fichiers, et découvrez des utilitaires importants pour les administrateurs Linux.

Système
Familiarisez-vous avec les composants de votre système Linux, ainsi qu'avec leurs interactions.

Services
Apprenez à configurer les différents services réseau et services de fichiers intégrés à SUSE Linux.

1 Commentaires

Vos remarques et suggestions sur ce manuel, ainsi que sur le reste de la documentation fournie avec ce produit, nous intéressent. Merci d'utiliser la fonction Commentaires, située au bas de chaque page de la documentation en ligne, ou accédez à la page `http://www.novell.com/documentation/feedback.html` et entrez vos commentaires.

2 Documentations supplémentaires

D'autres manuels relatifs à ce produit SUSE Linux sont disponibles ; vous pouvez y accéder en ligne, à l'adresse http://www.novell.com/documentation/, ou sur votre système, sous /usr/share/doc/manual/:

Démarrage
Ce manuel vous guide dans les premières étapes que vous réalisez avec SUSE Linux. Une version en ligne de ce document est disponible à l'adresse suivante : http://www.novell.com/documentation/suse10/.

Novell AppArmor Powered by Immunix 1.2 – Guide d'installation et de démarrage rapide
Ce guide décrit la procédure d'installation initiale du produit *AppArmor*. Une version en ligne de ce document est disponible à l'adresse suivante : http://www.novell.com/documentation/apparmor/.

Novell AppArmor Powered by Immunix 1.2 – Guide d'administration
Ce guide fournit des informations détaillées sur l'utilisation d'*AppArmor* dans votre environnement. Une version en ligne de ce document est disponible à l'adresse suivante : http://www.novell.com/documentation/apparmor/.

3 Conventions typographiques

Les conventions typographiques suivantes sont utilisées dans ce manuel :

- /etc/passwd : noms de fichiers et de répertoires
- *espace réservé* : remplacez *espace réservé* par la valeur réelle
- PATH : la variable d'environnement PATH
- ls, --help : commandes, options et paramètres
- utilisateur : utilisateurs ou groupes
- Alt, Alt + F1 : touche ou combinaison de touches sur lesquelles appuyer
- *Fichier*, *File* → *Enregistrer sous* : options de menu, boutons

- *Pingouins dansants* (Chapitre Pingouins, ↑*Référence*) : référence à un chapitre d'un autre ouvrage.

4 Remerciements

Très impliqués et volontaires, les développeurs de Linux travaillent ensemble, depuis les quatre coins du monde, au développement de Linux. Nous souhaitons les remercier pour leurs efforts ; cette diffusion n'existerait pas sans eux. Nos remerciements vont également à Frank Zappa et à Pawar. Nous remercions tout spécialement, bien sûr, Linus Torvalds.

À vous de jouer maintenant !

Votre équipe SUSE

Scénarios de déploiement avancés

1 Installation à distance

SUSE Linux peut être installé de différentes manières. Outre l'installation classique à partir d'un CD ou d'un DVD abordée au Chapitre *Installation avec YaST* (↑Démarrage), vous avez le choix entre différentes approches réseau, et pouvez même envisager une approche entièrement automatique de l'installation de SUSE Linux.

En introduction de chaque méthode figurent deux brèves listes de contrôle : l'une répertorie les conditions préalables à cette méthode et l'autre reprend la procédure de base. Des informations supplémentaires vous sont ensuite fournies pour toutes les techniques utilisées dans ces scénarios d'installation.

REMARQUE

Dans les sections suivantes, le système destiné à héberger votre nouvelle installation SUSE Linux est appelé *système cible* ou *cible d'installation*. Le terme *source d'installation* désigne toutes les sources de données d'installation. Il s'agit notamment des supports physiques, tels que les CD et DVD, et des serveurs réseau qui transfèrent les données d'installation sur votre réseau.

1.1 Scénarios d'installation à distance

Cette section présente les scénarios d'installation à distance les plus courants. Pour chaque scénario, vérifiez soigneusement la liste des conditions préalables et suivez la

procédure correspondante. Si vous avez besoin d'instructions détaillées pour une étape précise, cliquez sur les liens fournis à cet effet.

IMPORTANT

La configuration du système X Window ne fait partie d'aucun processus d'installation à distance. À la fin de l'installation, loguez-vous au système cible en tant qu'utilisateur root, entrez `init 3` et démarrez SaX2 pour configurer le matériel graphique, comme décrit à la Section 35.1, « Configuration de X11 avec SaX2 » (p. 563).

1.1.1 Installation à distance simple via VNC : configuration réseau statique

Ce type d'installation nécessite toujours un certain niveau d'accès physique au système cible pour démarrer l'installation. L'installation même est entièrement contrôlée par un poste de travail distant qui utilise VNC pour se connecter au programme d'installation. Une intervention de l'utilisateur est nécessaire, comme pour l'installation manuelle décrite dans le Chapitre *Installation avec YaST* (↑Démarrage).

Pour ce type d'installation, assurez-vous de respecter les exigences suivantes :

- source de l'installation à distance : NFS, HTTP, FTP ou SMB avec connexion réseau établie ;
- système cible avec connexion réseau établie ;
- système de contrôle avec connexion réseau établie, et logiciel de visualisation VNC ou navigateur Java (Firefox, Konqueror, Internet Explorer ou Opera) ;
- support de démarrage physique (CD ou DVD) pour l'amorçage du système cible ;
- adresses IP statiques valides déjà affectées à la source d'installation et au système de contrôle ;
- adresse IP statique valide à affecter au système cible.

Pour effectuer ce type d'installation, procédez comme suit :

1 Configurez la source d'installation en suivant la procédure décrite à la Section 1.2, « Configuration du serveur qui contient les sources d'installation » (p. 31).

2 Démarrez le système cible en utilisant le premier CD ou DVD du kit de support SUSE Linux.

3 Lorsque l'écran de démarrage du système cible apparaît, utilisez l'invite de saisie des options de démarrage pour définir les options VNC appropriées et l'adresse de la source d'installation. Cette opération est décrite en détail à la Section 1.4, « Démarrage du système cible pour l'installation » (p. 52).

   Le système cible démarre dans un environnement texte, qui indique l'adresse réseau et le numéro d'affichage grâce auxquels toute application de visualisation VNC ou tout navigateur peut contacter l'environnement d'installation graphique. Les installations VNC s'annoncent via OpenSLP et peuvent être trouvées à l'aide de Konqueror en mode `service://` ou `slp://`.

4 Sur le poste de travail de contrôle, ouvrez une application de visualisation VNC ou un navigateur Web et connectez-vous au système cible, comme décrit à la Section 1.5.1, « Installation VNC » (p. 57).

5 Effectuez l'installation en suivant la procédure décrite au Chapitre *Installation avec YaST* (↑Démarrage) .

   Pour la dernière partie de l'installation, vous devrez vous reconnecter au système cible après son redémarrage.

6 Achevez l'installation.

1.1.2 Installation à distance simple via VNC : configuration réseau dynamique via DHCP

Ce type d'installation nécessite toujours un certain niveau d'accès physique au système cible pour démarrer l'installation. La configuration du réseau s'effectue à l'aide du protocole DHCP. L'installation même est entièrement contrôlée à partir d'un poste de travail distant qui utilise VNC pour se connecter au programme d'installation ; elle

nécessite toujours une intervention de l'utilisateur pour les besoins de configuration réels.

Pour ce type d'installation, assurez-vous de respecter les exigences suivantes :

- source de l'installation à distance : NFS, HTTP, FTP ou SMB avec connexion réseau établie ;
- système cible avec connexion réseau établie ;
- système de contrôle avec connexion réseau établie, et logiciel de visualisation VNC ou navigateur Java (Firefox, Konqueror, Internet Explorer ou Opera) ;
- support de démarrage physique (CD, DVD, disque de démarrage personnalisé) pour l'amorçage du système cible ;
- serveur DHCP en cours d'exécution qui fournit des adresses IP.

Pour effectuer ce type d'installation, procédez comme suit :

1. Configurez la source d'installation en suivant la procédure décrite à la Section 1.2, « Configuration du serveur qui contient les sources d'installation » (p. 31). Choisissez un serveur réseau NFS, HTTP ou FTP. Pour une source d'installation SMB, consultez la Section 1.2.5, « Gestion d'une source d'installation SMB » (p. 40).

2. Démarrez le système cible en utilisant le premier CD ou DVD du kit de support SUSE Linux.

3. Lorsque l'écran de démarrage du système cible apparaît, utilisez l'invite de saisie des options de démarrage pour définir les options VNC appropriées et l'adresse de la source d'installation. Cette opération est décrite en détail à la Section 1.4, « Démarrage du système cible pour l'installation » (p. 52).

   Le système cible démarre dans un environnement texte, qui indique l'adresse réseau et le numéro d'affichage grâce auxquels toute application de visualisation VNC ou tout navigateur peut contacter l'environnement d'installation graphique. Les installations VNC s'annoncent via OpenSLP et peuvent être trouvées à l'aide de Konqueror en mode `service://` ou `slp://`.

4 Sur le poste de travail de contrôle, ouvrez une application de visualisation VNC ou un navigateur Web et connectez-vous au système cible, comme décrit à la Section 1.5.1, « Installation VNC » (p. 57).

5 Effectuez l'installation en suivant la procédure décrite au Chapitre *Installation avec YaST* (↑Démarrage) .

   Pour la dernière partie de l'installation, vous devrez vous reconnecter au système cible après son redémarrage.

6 Achevez l'installation.

1.1.3 Installation à distance via VNC : démarrage PXE et fonction Wake on LAN (réveil à distance)

Ce type d'installation est entièrement automatique. La machine cible est démarrée et amorcée à distance. L'intervention de l'utilisateur n'est nécessaire que pour l'installation réelle. Cette approche est adaptée aux opérations de déploiement sur plusieurs sites.

Pour effectuer ce type d'installation, assurez-vous de respecter les contraintes suivantes :

- source de l'installation à distance : NFS, HTTP, FTP ou SMB avec connexion réseau établie ;
- serveur TFTP ;
- serveur DHCP en cours d'exécution pour votre réseau ;
- système cible, branché et connecté au réseau, qui dispose d'une fonction de démarrage PXE, d'une prise en charge réseau et d'une fonction Wake on LAN ;
- système de contrôle avec connexion réseau établie et logiciel de visualisation VNC du navigateur Java (Firefox, Konqueror, Internet Explorer ou Opera).

Pour effectuer ce type d'installation, procédez comme suit :

1 Configurez la source d'installation en suivant la procédure décrite à la Section 1.2, « Configuration du serveur qui contient les sources d'installation » (p. 31).

Choisissez un serveur réseau NFS, HTTP ou FTP, ou configurez une source d'installation SMB en suivant la procédure décrite à la Section 1.2.5, « Gestion d'une source d'installation SMB » (p. 40).

2 Configurez un serveur TFTP de manière à ce qu'il contienne une image de démarrage qui peut être extraite par le système cible. Cette opération est décrite à la Section 1.3.2, « Configuration d'un serveur TFTP » (p. 43).

3 Configurez un serveur DHCP de manière à fournir des adresses IP à toutes les machines et indiquez l'emplacement du serveur TFTP au système cible. Cette opération est décrite à la Section 1.3.1, « Configuration d'un serveur DHCP » (p. 42).

4 Préparez le système cible pour le démarrage PXE. Cette opération est décrite plus en détail à la Section 1.3.5, « Préparation du système cible pour le démarrage PXE » (p. 50).

5 Lancez le processus de démarrage du système cible à l'aide de la fonction Wake on LAN. Cette opération est décrite à la Section 1.3.7, « Wake on LAN (réveil à distance) » (p. 51).

6 Sur le poste de travail de contrôle, ouvrez une application de visualisation VNC ou un navigateur Web et connectez-vous au système cible, comme décrit à la Section 1.5.1, « Installation VNC » (p. 57).

7 Effectuez l'installation en suivant la procédure décrite au Chapitre *Installation avec YaST* (↑Démarrage) .

   Pour la dernière partie de l'installation, vous devrez vous reconnecter au système cible après son redémarrage.

8 Achevez l'installation.

1.1.4 Installation à distance simple via SSH : configuration réseau statique

Ce type d'installation nécessite toujours un certain niveau d'accès physique au système cible pour démarrer l'installation et déterminer l'adresse IP de la cible d'installation. L'installation même est entièrement contrôlée à partir d'un poste de travail distant qui

utilise le protocole SSH pour se connecter au programme d'installation. Une intervention de l'utilisateur est nécessaire, comme pour l'installation standard décrite dans le Chapitre *Installation avec YaST* (↑Démarrage).

Pour ce type d'installation, assurez-vous de respecter les exigences suivantes :

- source de l'installation à distance : NFS, HTTP, FTP ou SMB avec connexion réseau établie ;
- système cible avec connexion réseau établie ;
- système de contrôle avec connexion réseau établie, et logiciel de visualisation VNC ou navigateur Java (Firefox, Konqueror, Internet Explorer ou Opera) ;
- support de démarrage physique (CD, DVD, disque de démarrage personnalisé) pour le système cible ;
- adresses IP statiques valides déjà affectées à la source d'installation et au système de contrôle ;
- adresse IP statique valide à affecter au système cible.

Pour effectuer ce type d'installation, procédez comme suit :

1. Configurez la source d'installation en suivant la procédure décrite à la Section 1.2, « Configuration du serveur qui contient les sources d'installation » (p. 31).

2. Démarrez le système cible en utilisant le premier CD ou DVD du kit de support SUSE Linux.

3. Lorsque l'écran de démarrage du système cible apparaît, utilisez l'invite de saisie des options de démarrage pour définir les paramètres adaptés à la connexion réseau, l'adresse de la source d'installation et l'activation de la fonctionnalité SSH. Cette opération est décrite en détail à la Section 1.4.3, « Utilisation des options de démarrage personnalisées » (p. 54).

   Le système cible démarre dans un environnement texte, qui indique l'adresse réseau et le numéro d'affichage grâce auxquels tout client SSH peut contacter l'environnement d'installation graphique.

4 Sur le poste de travail de contrôle, ouvrez une fenêtre de terminal et connectez-vous au système cible, comme décrit à la section intitulée « Connexion au programme d'installation » (p. 60).

5 Effectuez l'installation en suivant la procédure décrite au Chapitre *Installation avec YaST* (↑Démarrage) .

   Pour la dernière partie de l'installation, vous devrez vous reconnecter au système cible après son redémarrage.

6 Achevez l'installation.

1.1.5 Installation à distance simple via SSH : configuration réseau dynamique via DHCP

Ce type d'installation nécessite toujours un certain niveau d'accès physique au système cible pour démarrer l'installation et déterminer l'adresse IP de la cible d'installation. L'installation même est entièrement contrôlée à partir d'un poste de travail distant qui utilise VNC pour se connecter au programme d'installation ; elle nécessite toujours une intervention de l'utilisateur pour les besoins de configuration réels.

Pour ce type d'installation, assurez-vous de respecter les exigences suivantes :

- source de l'installation à distance : NFS, HTTP, FTP ou SMB avec connexion réseau établie ;
- système cible avec connexion réseau établie ;
- système de contrôle avec connexion réseau établie, et logiciel de visualisation VNC ou navigateur Java (Firefox, Konqueror, Internet Explorer ou Opera) ;
- support de démarrage physique (CD ou DVD) pour l'amorçage du système cible ;
- serveur DHCP en cours d'exécution qui fournit des adresses IP.

Pour effectuer ce type d'installation, procédez comme suit :

1 Configurez la source d'installation en suivant la procédure décrite à la Section 1.2, « Configuration du serveur qui contient les sources d'installation » (p. 31). Choisissez un serveur réseau NFS, HTTP ou FTP. Pour une source d'installation SMB, consultez la Section 1.2.5, « Gestion d'une source d'installation SMB » (p. 40).

2 Démarrez le système cible en utilisant le premier CD ou DVD du kit de support SUSE Linux.

3 Lorsque l'écran de démarrage du système cible apparaît, utilisez l'invite de saisie des options de démarrage pour transmettre les paramètres adaptés à la connexion réseau, l'emplacement de la source d'installation et l'activation de la fonctionnalité SSH. Pour obtenir des instructions détaillées sur l'utilisation de ces paramètres, consultez la Section 1.4.3, « Utilisation des options de démarrage personnalisées » (p. 54).

   Le système cible démarre dans un environnement texte, qui vous indique l'adresse réseau grâce à laquelle tout client SSH peut contacter l'environnement d'installation graphique.

4 Sur le poste de travail de contrôle, ouvrez une fenêtre de terminal et connectez-vous au système cible, comme décrit à la section intitulée « Connexion au programme d'installation » (p. 60).

5 Effectuez l'installation en suivant la procédure décrite au Chapitre *Installation avec YaST* (↑Démarrage) .

   Pour la dernière partie de l'installation, vous devrez vous reconnecter au système cible après son redémarrage.

6 Achevez l'installation.

1.1.6 Installation à distance via SSH : démarrage PXE et fonction Wake on LAN (réveil à distance)

Ce type d'installation est entièrement automatique. La machine cible est démarrée et amorcée à distance.

Pour effectuer ce type d'installation, assurez-vous de respecter les contraintes suivantes :

- source de l'installation à distance : NFS, HTTP, FTP ou SMB avec connexion réseau établie ;
- serveur TFTP ;
- serveur DHCP en cours d'exécution pour votre réseau, qui fournit une adresse IP statique à l'hôte qui doit être installé ;
- système cible, branché et connecté au réseau, qui dispose d'une fonction de démarrage PXE, d'une prise en charge réseau et d'une fonction Wake on LAN ;
- système de contrôle doté d'une connexion réseau établie et d'un logiciel client SSH

Pour effectuer ce type d'installation, procédez comme suit :

1. Configurez la source d'installation en suivant la procédure décrite à la Section 1.2, « Configuration du serveur qui contient les sources d'installation » (p. 31). Choisissez un serveur réseau NFS, HTTP ou FTP. Pour la configuration d'une source d'installation SMB, consultez la Section 1.2.5, « Gestion d'une source d'installation SMB » (p. 40).

2. Configurez un serveur TFTP de manière à ce qu'il contienne une image de démarrage qui peut être extraite par le système cible. Cette opération est décrite à la Section 1.3.2, « Configuration d'un serveur TFTP » (p. 43).

3. Configurez un serveur DHCP de manière à fournir des adresses IP à toutes les machines et indiquez l'emplacement du serveur TFTP au système cible. Cette opération est décrite à la Section 1.3.1, « Configuration d'un serveur DHCP » (p. 42).

4. Préparez le système cible pour le démarrage PXE. Cette opération est décrite plus en détail à la Section 1.3.5, « Préparation du système cible pour le démarrage PXE » (p. 50).

5. Lancez le processus de démarrage du système cible à l'aide de la fonction Wake on LAN. Cette opération est décrite à la Section 1.3.7, « Wake on LAN (réveil à distance) » (p. 51).

6 Sur le poste de travail de contrôle, démarrez un client VNC et connectez-vous au système cible, comme décrit à la section intitulée « Connexion au programme d'installation » (p. 60).

7 Effectuez l'installation en suivant la procédure décrite au Chapitre *Installation avec YaST* (↑Démarrage) .

   Pour la dernière partie de l'installation, vous devrez vous reconnecter au système cible après son redémarrage.

8 Achevez l'installation.

1.2 Configuration du serveur qui contient les sources d'installation

En fonction du système d'exploitation qui s'exécute sur la machine à utiliser comme source d'installation réseau pour SUSE Linux, plusieurs options sont disponibles pour la configuration du serveur. La méthode la plus simple pour configurer un serveur d'installation consiste à utiliser YaST sur SUSE LINUX Enterprise Server 9, ou SUSE Linux 9.3 et versions ultérieures. Sur les autres versions de SUSE LINUX Enterprise Server ou SUSE Linux, configurez la source d'installation manuellement.

ASTUCE

Vous pouvez même utiliser une machine Microsoft Windows comme serveur d'installation pour le déploiement de Linux. Pour plus de détails, consultez la Section 1.2.5, « Gestion d'une source d'installation SMB » (p. 40).

1.2.1 Configuration d'un serveur d'installation à l'aide de YaST

YaST fournit un outil graphique qui permet de créer des sources d'installation réseau. Il prend en charge les serveurs d'installation réseau HTTP, FTP et NFS.

1 Loguez-vous en tant qu'utilisateur root à la machine qui doit jouer le rôle de serveur d'installation.

2 Démarrez *YaST* → *Divers* → *Serveur d'installation*.

3 Sélectionnez le type de serveur (HTTP, FTP ou NFS).

Le service de serveur sélectionné est démarré automatiquement à chaque démarrage du système. Si un service du type sélectionné est déjà en cours d'exécution sur votre système et si vous souhaitez le configurer manuellement, désactivez la fonction de configuration automatique du service de serveur en sélectionnant *Ne configurer aucun des services réseau*. Dans les deux cas, définissez le répertoire du serveur dans lequel placer les données d'installation.

4 Configurez le type de serveur nécessaire.

Cette étape concerne la configuration automatique des services de serveur. Elle est ignorée lorsque la configuration automatique est désactivée. Définissez un alias pour le répertoire racine du serveur FTP ou HTTP sur lequel les données d'installation doivent figurer. La source d'installation sera ultérieurement située sous`ftp://`*`IP-serveur/Alias/Nom`* (FTP) ou sous `http://`*`IP-serveur/Alias/Nom`* (HTTP). *`Nom`* désigne le nom de la source d'installation, dont la définition s'effectue à l'étape suivante. Si vous avez sélectionné NFS à l'étape précédente, définissez des caractères joker et des options d'exportation. Le serveur NFS sera accessible sous `nfs://`*`IP-serveur/Nom`* . Pour plus d'informations sur le serveur NFS et les exportations, consultez le Chapitre 42, *Partage des systèmes de fichiers avec NFS* (p. 685).

5 Configurez la source d'installation.

Avant la copie des supports d'installation vers leur destination, définissez le nom de la source d'installation (choisissez plutôt une abréviation du produit et de la version facile à mémoriser). YaST permet de fournir des images ISO des supports au lieu des copies des CD d'installation. Pour ce faire, sélectionnez la case à cocher correspondante et indiquez le chemin du répertoire sous lequel trouver les fichiers ISO localement. En fonction du produit à distribuer à l'aide du serveur d'installation, vous pouvez avoir besoin d'un plus grand nombre de CD de modules complémentaires ou de CD de service pack pour installer entièrement le produit. Si vous sélectionnez *Invite pour des CD additionnels*, YaST vous rappelle automatiquement de fournir les supports en question. Pour annoncer votre serveur d'installation sur le réseau via OpenSLP, sélectionnez l'option correspondante.

ASTUCE

Pensez à annoncer votre source d'installation via OpenSLP si la configuration du réseau prend en charge cette option. Cela vous évite d'entrer le chemin d'installation réseau sur chaque machine cible. Les systèmes cible sont simplement démarrés à l'aide de l'option d'amorçage SLP ; ils trouveront la source d'installation réseau sans qu'aucune autre opération de configuration ne soit nécessaire. Pour plus d'informations sur cette option, consultez la Section 1.4, « Démarrage du système cible pour l'installation » (p. 52).

6 Téléchargez les données d'installation.

La copie des CD d'installation constitue l'étape la plus longue dans la configuration d'un serveur d'installation. Insérez les supports dans l'ordre demandé par YaST et attendez la fin de la procédure de copie. Lorsque les sources ont été entièrement copiées, revenez à l'aperçu des sources d'informations existantes et fermez la configuration en sélectionnant *Terminer*.

Le serveur d'installation est désormais entièrement configuré et prêt à fonctionner. Il démarre automatiquement en même temps que le système. Aucune autre intervention n'est nécessaire. Si vous avez désactivé à l'aide de YaST la configuration automatique du service réseau sélectionné lors de la première étape, il vous suffit de configurer et de démarrer manuellement ce service.

Pour désactiver une source d'installation, sélectionnez *Modifier* dans l'aperçu pour ouvrir la liste des sources d'installation disponibles. Choisissez l'entrée à supprimer, puis cliquez sur *Supprimer*. Cette procédure de suppression ne concerne que la désactivation du service de serveur. Les données d'installation restent dans le répertoire choisi. Cependant, vous pouvez les supprimer manuellement.

Si votre serveur d'installation doit fournir les données d'installation pour plus d'un produit de cette version, démarrez le module de serveur d'installation YaST et sélectionnez *Configurer* dans l'aperçu des sources d'installation existantes pour configurer la nouvelle source d'installation.

1.2.2 Installation manuelle d'une source d'installation NFS

La configuration d'une source NFS en vue d'une opération d'installation s'effectue généralement en deux étapes. Dans un premier temps, créez l'arborescence qui contient les données d'installation et copiez les supports d'installation vers cette arborescence. Exportez ensuite le répertoire qui contient les données d'installation vers le réseau.

Pour créer un répertoire qui contient les données d'installation, procédez comme suit :

1 Loguez-vous en tant qu'utilisateur root.

2 Créez un répertoire destiné à contenir les données d'installation et accédez à ce répertoire. Par exemple :

```
mkdir install/produit/versionproduit
```

```
cd install/produit/versionproduit
```

Remplacez `produit` par une abréviation du nom du produit (dans le cas présent, SUSE Linux) et `versionproduit` par une chaîne qui contient le nom et la version du produit.

3 Pour chaque CD contenu dans le kit de support, exécutez les commandes suivantes :

a Copiez tout le contenu du CD d'installation vers le répertoire du serveur d'installation :

```
cp -a /media/chemin_de_votre_lecteur_CD-ROM.
```

Remplacez `chemin_de_votre_lecteur_CD-ROM` par le chemin réel qui permet d'accéder au lecteur de CD ou DVD. En fonction du type de lecteur utilisé dans le système, il peut s'agir de `cdrom`, `cdrecorder`, `dvd` ou `dvdrecorder`.

b Renommez le répertoire en incluant le numéro de CD :

```
mv chemin_de_votre_lecteur_CD-ROM CDx
```

Remplacez *x* par le numéro réel de votre CD.

Pour exporter, via le serveur NFS, les sources d'installation à l'aide de YaST, procédez comme suit :

1 Loguez-vous en tant qu'utilisateur root.

2 Sélectionnez *YaST* → *Services réseau* → *Serveur NFS*.

3 Cliquez sur *Démarrer le serveur NFS* et *Ouvrir port dans pare-feu*, puis cliquez sur *Suivant*.

4 Sélectionnez *Ajouter répertoire* et entrez le chemin du répertoire qui contient les données d'installation. Dans ce cas, il s'agit de `/`*`versionproduit`*.

5 Sélectionnez *Ajouter hôte* et entrez les noms d'hôte des machines vers lesquelles exporter les données d'installation. Au lieu d'indiquer les noms d'hôte, vous pouvez également utiliser des caractères joker, des plages d'adresses réseau ou simplement le nom de domaine de votre réseau. Entrez les options d'exportation appropriées ou laissez celles par défaut ; ces dernières fonctionnent correctement dans la plupart des configurations. Pour plus d'informations sur la syntaxe utilisée lors de l'exportation des partages NFS, consultez la page d'aide consacrée à l'`exportation`.

6 Cliquez sur *Terminer*.

Le serveur NFS qui contient les sources d'installation de SUSE Linux est démarré et intégré automatiquement au processus d'amorçage.

Si vous préférez exporter manuellement les sources d'installation via NFS plutôt que d'utiliser le module de serveur NFS de YaST, procédez comme suit :

1 Loguez-vous en tant qu'utilisateur root.

2 Ouvrez le fichier `/etc/exports` et entrez la ligne de commande suivante :

```
/versionproduit *(ro,root_squash,sync)
```

Cette commande permet d'exporter le répertoire `/`*`versionproduit`* vers tout hôte membre de ce réseau ou capable de se connecter à ce serveur. Pour limiter l'accès à ce serveur, remplacez le caractère joker générique `*` par des masques de réseau ou des noms de domaine. Pour plus d'informations, consultez la page

d'aide consacrée à l'`exportation`. Enregistrez et quittez ce fichier de configuration.

3 Pour ajouter le service NFS à la liste des serveurs démarrés au cours de l'amorçage du système, exécutez les commandes suivantes :

```
insserv /etc/init.d/nfsserver
```

```
insserv /etc/init.d/portmap
```

4 Démarrez le serveur NFS à l'aide de la commande suivante :

```
rcnfsserver start
```

Si, ultérieurement, vous devez changer la configuration de votre serveur NFS, modifiez le fichier de configuration et redémarrez le démon NFS à l'aide de la commande `rcnfsserver restart`.

L'annonce du serveur NFS via OpenSLP permet de communiquer l'adresse de ce serveur à tous les clients du réseau.

1 Loguez-vous en tant qu'utilisateur root.

2 Accédez au répertoire `/etc/slp.reg.d/`.

3 Créez un fichier de configuration nommé `install.suse.nfs.reg` qui contient les lignes suivantes :

```
# Enregistrement du serveur d'installation NFS
service:install.suse:nfs://$HOSTNAME/chemin_sourceinst/CD1,en,65535
description=source d'installation NFS
```

Remplacez *`chemin_sourceinst`* par le chemin réel de la source d'installation sur votre serveur.

4 Enregistrez ce fichier de configuration et démarrez le démon OpenSLP à l'aide de la commande suivante :

```
rcslpd start
```

Pour plus d'informations sur OpenSLP, consultez la documentation relative au paquetage, située dans `/usr/share/doc/packages/openslp/`, ou le Chapitre 39, *Services SLP sur le réseau* (p. 651).

1.2.3 Configuration manuelle d'une source d'installation FTP

La création d'une source d'installation FTP est très semblable à celle d'une source d'installation NFS. Les sources d'installation FTP peuvent également être annoncées sur le réseau à l'aide d'OpenSLP.

1. Créez un répertoire qui contient les sources d'installation en suivant la procédure décrite à la Section 1.2.2, « Installation manuelle d'une source d'installation NFS » (p. 34).

2. Configurez le serveur FTP pour distribuer le contenu de votre répertoire d'installation :

   a. Loguez-vous en tant qu'utilisateur root et installez le paquetage `pure-ftpd` (serveur FTP léger) à l'aide du gestionnaire de paquetages YaST.

   b. Entrez dans le répertoire racine du serveur FTP :

   ```
   cd/srv/ftp
   ```

   c. Créez un sous-répertoire qui contient les sources d'installation dans le répertoire racine FTP :

   ```
   mkdirsourceinst
   ```

   Remplacez *`sourceinst`* par le nom du produit.

   d. Copiez le contenu des CD d'installation dans le répertoire racine du serveur FTP (procédure semblable à celle décrite dans la Section 1.2.2, « Installation manuelle d'une source d'installation NFS » (p. 34), Étape 3 (p. 34)).

   Vous pouvez également monter le contenu du référentiel d'installation existant dans l'environnement racine modifié du serveur FTP :

   ```
   mount --bind
   chemin_de_sourceinst /srv/ftp/sourceinst
   ```

Remplacez les variables *chemin_de_sourceinst* et *sourceinst* par des valeurs adaptées à votre configuration. Pour que ces modifications soient permanentes, ajoutez-les au fichier /etc/fstab.

e Démarrez pure-ftpd :

```
pure-ftpd &
```

3 Annoncez la source d'installation via OpenSLP, si votre configuration réseau prend en charge cette opération :

a Créez un fichier de configuration nommé install.suse.ftp.reg dans /etc/slp/reg.d/ en incluez-y les lignes suivantes :

```
# Enregistrement du serveur d'installation FTP
service:install.suse:ftp://$HOSTNAME/srv/ftp/sourceinst/CD1,en,65535
description=source d'installation FTP
```

Remplacez *sourceinst* par le nom réel du répertoire de la source d'installation de votre serveur. La ligne service: doit être entrée sous forme de ligne continue.

b Enregistrez ce fichier de configuration et démarrez le démon OpenSLP à l'aide de la commande suivante :

```
rcslpd start
```

1.2.4 Installation manuelle d'une source d'installation HTTP

La création d'une source d'installation HTTP est très semblable à celle d'une source d'installation NFS. Les sources d'installation HTTP peuvent également être annoncées sur le réseau à l'aide d'OpenSLP.

1 Créez un répertoire qui contient les sources d'installation en suivant la procédure décrite à la Section 1.2.2, « Installation manuelle d'une source d'installation NFS » (p. 34).

2 Configurez le serveur HTTP pour distribuer le contenu de votre répertoire d'installation :

a Loguez-vous en tant qu'utilisateur root et installez le paquetage `apache2` à l'aide du gestionnaire de paquetages YaST.

b Accédez au répertoire racine du serveur HTTP (`/srv/www/htdocs`) et créez un sous-répertoire qui contiendra les sources d'installation :

```
mkdir sourceinst
```

Remplacez *`sourceinst`* par le nom du produit.

c Créez un lien symbolique à partir de l'emplacement des sources d'installation vers le répertoire racine du serveur Web (`/srv/www/htdocs`) :

```
ln -s /chemin_sourceinst /srv/www/htdocs/sourceinst
```

d Modifiez le fichier de configuration du serveur HTTP (`/etc/apache2/default-server.conf`) de manière à ce qu'il suive les liens symboliques. Remplacez la ligne suivante :

```
Options None
```

par

```
Options Indexes FollowSymLinks
```

e Redémarrez le serveur HTTP à l'aide de la commande `rcapache2 restart`.

3 Annoncez la source d'installation via OpenSLP, si votre configuration réseau prend en charge cette opération :

a Créez un fichier de configuration nommé `install.suse.http.reg` dans `/etc/slp/reg.d/` en incluez-y les lignes suivantes :

```
# Enregistrement du serveur d'installation HTTP
service:install.suse:http://$HOSTNAME/svr/www/htdocs/sourceinst/CD1,en,65535
description=source d'installation HTTP
```

Remplacez *`chemin_de_sourceinst`* par le chemin réel de la source d'installation de votre serveur. La ligne `service:` doit être entrée sous forme de ligne continue.

b Enregistrez ce fichier de configuration et démarrez le démon OpenSLP à l'aide de la commande `rcslpd restart`.

1.2.5 Gestion d'une source d'installation SMB

À l'aide du protocole SMB (Samba), vous pouvez importer les sources d'installation depuis un serveur Microsoft Windows et démarrer le déploiement Linux sans même disposer d'une machine Linux.

Pour configurer un partage Windows exporté où sont stockées vos sources d'installation SUSE Linux, procédez comme suit :

1. Loguez-vous à votre machine Windows.

2. Démarrez l'Explorateur, créez un répertoire qui contiendra l'intégralité de l'arborescence d'installation et nommez-le `INSTALL`, par exemple.

3. Exportez ce partage en suivant la procédure décrite dans votre documentation Windows.

4. Accédez à ce partage et créez un sous-répertoire nommé *`produit`*. Remplacez la variable *`produit`* par le nom réel du produit (SUSE Linux dans ce cas).

5. Copiez chaque CD SUSE Linux vers un répertoire distinct et nommez-les `CD1`, `CD2`, `CD3`, etc.

6. Entrez dans le répertoire de niveau supérieur du partage exporté (`INSTALL` dans cet exemple), puis copiez les fichiers et répertoires suivants depuis *`produit`*`/CD1` vers ce répertoire : `content`, `media.1`, `control.xml` et `boot`.

7. Créez un répertoire sous `INSTALL` et nommez-le `yast`.

8. Accédez au répertoire `yast` et créez les fichiers `order` et `instorder`.

9. Ouvrez le fichier `order` et entrez la ligne suivante :

```
/NLD/CD1 smb://utilisateur:motdepasse@nomhôte/produitCD1
```

Remplacez *utilisateur* par le nom d'utilisateur entré sur la machine Windows ou utilisez la valeur `Guest` pour permettre une connexion en tant qu'invité à ce partage. Remplacez la variable *motdepasse* par votre mot de passe de connexion ou par une autre chaîne dans le cadre d'une connexion en tant qu'invité. *nomhôte* correspond au nom de réseau de votre machine Windows.

- Ouvrez le fichier `instorder` et ajoutez la ligne suivante :

```
/produit/CD1
```

Pour utiliser un partage monté SMB comme source d'installation, procédez comme suit :

1. Démarrez la cible d'installation.

2. Sélectionnez *Installation*.

3. Appuyez sur la touche F4 pour sélectionner les sources d'installation.

4. Choisissez SMB, et entrez le nom ou l'adresse IP de la machine Windows, le nom du partage (`INSTALL` dans cet exemple), le nom d'utilisateur et le mot de passe.

   Une fois que vous avez appuyé sur Entrée, YaST démarre et vous pouvez effectuer l'installation.

1.3 Préparation du démarrage du système cible

Cette section expose les tâches de configuration nécessaires pour les scénarios de démarrage complexes. Elle contient des exemples de configuration « prêts à l'emploi » pour le protocole DHCP, le démarrage PXE, le protocole TFTP et la fonction Wake on LAN.

1.3.1 Configuration d'un serveur DHCP

Pour configurer un serveur DHCP sur SUSE Linux, vous devez modifier manuellement les fichiers de configuration appropriés. Cette section explique également comment étendre une configuration de serveur DHCP existante dans le but de fournir les données nécessaires à un environnement TFTP, PXE et WOL.

Configuration manuelle d'un serveur DHCP

Le serveur DHCP n'a qu'une chose à faire, à part fournir une allocation d'adresse automatique aux clients du réseau : déclarer l'adresse IP du serveur TFTP et le fichier qui doit être utilisé par les routines d'installation sur la machine cible.

1. Loguez-vous en tant qu'utilisateur root à la machine qui héberge le serveur DHCP.

2. Ajoutez les lignes suivantes dans le fichier de configuration du serveur DHCP situé sous `/etc/dhcpd.conf` :

   ```
   group {
    # Informations relatives à PXE
    #
    # "serveur suivant" définit le serveur tftp qui sera utilisé
    après le serveur ip_serveur_tftp:
    #
    # "nom de fichier" indique l'image pxelinux sur le serveur tftp
    # le serveur s'exécute en mode chroot sous /srv/tftpboot
    filename  "pxelinux.0";
   }
   ```

   Remplacez *`ip_du_serveur_tftpr`* par l'adresse IP réelle du serveur TFTP.

   Pour plus d'informations sur les options disponibles dans`dhcpd.conf`, consultez la page d'aide `dhcpd.conf`.

3. Redémarrez le serveur DHCP en exécutant la commande `rcdhcpd restart`

Si vous avez l'intention d'utiliser le protocole SSH pour le contrôle distant d'une installation PXE et Wake on LAN, indiquez de manière explicite l'adresse IP que le protocole DHCP doit fournir à la cible d'installation. Pour ce faire, modifiez la configuration DHCP mentionnée ci-dessus, conformément à l'exemple suivant :

```
group {
 # Informations relatives à PXE
```

```
#
# "serveur suivant" définit le serveur tftp qui sera utilisé
après le serveur ip_serveur_tftp:
#
# "nom de fichier" indique l'image pxelinux sur le serveur tftp
# le serveur s'exécute en mode chroot sous /srv/tftpboot
filename  "pxelinux.0";
host test { hardware ethernet adresse_mac;
 fixed-address une_adresse_ip; }
}
```

L'instruction d'hôte présente le nom d'hôte de la cible d'installation. Pour lier le nom d'hôte et l'adresse IP à un hôte particulier, vous devez connaître et indiquer l'adresse matérielle du système (MAC). Remplacez toutes les variables utilisées dans cet exemple par les valeurs réelles qui correspondent à votre environnement.

Une fois le serveur DHCP redémarré, une adresse IP statique est fournie à l'hôte spécifié ; vous pouvez ainsi vous connecter au système via la fonctionnalité SSH.

1.3.2 Configuration d'un serveur TFTP

Vous pouvez configurer un serveur TFTP en utilisant YaST ou manuellement sur tout autre système d'exploitation Linux qui prend en charge xinetd et tftp. Le serveur TFTP fournit l'image de démarrage au système cible lorsque ce dernier démarre et envoie une requête à ce sujet.

Configuration d'un serveur TFTP à l'aide de YaST

1. Loguez-vous en tant qu'utilisateur root.

2. Sélectionnez *YaST* → *Services réseau* → *Serveur TFTP* et installez le paquetage demandé.

3. Cliquez sur *Activer* pour vous assurer que le serveur est démarré et inclus dans les routines de démarrage. Aucune autre action de votre part n'est nécessaire pour vérifier la réussite de cette opération. xinetd démarre tftpd au moment de l'amorçage.

4. Cliquez sur *Ouvrir port dans pare-feu* pour ouvrir le port approprié dans le pare-feu exécuté sur votre machine. Si aucun pare-feu n'est en cours d'exécution sur votre serveur, cette option n'est pas disponible.

5 Cliquez sur *Parcourir* pour rechercher le répertoire de l'image de démarrage.

Le répertoire par défaut `/tftpboot` est créé et sélectionné automatiquement.

6 Cliquez sur *Terminer* pour appliquer vos paramètres et démarrer le serveur.

Configuration manuelle d'un serveur TFTP

1 Loguez-vous en tant qu'utilisateur root, et installez les paquetages `tftp` et `xinetd`.

2 S'ils ne sont pas disponibles, créez les répertoires `/srv/tftpboot` et `/srv/tftpboot/pxelinux.cfg`.

3 Ajoutez les fichiers nécessaires à l'image de démarrage, comme décrit dans la Section 1.3.3, « Démarrage PXE » (p. 45).

4 Modifiez la configuration de xinetd, situé sous `/etc/xinetd.d/`, pour vous assurer que le serveur tftp démarre à l'amorçage :

a S'il n'existe pas, créez dans ce répertoire un fichier nommé `tftp`, à l'aide de la commande `touch tftp`. Exécutez ensuite `chmod 755 tftp`.

b Ouvrez le fichier `tftp` et ajoutez les lignes suivantes :

```
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
        disable                 = no
}
```

c Enregistrez le fichier et redémarrez xinetd en exécutant `rcxinetd restart`.

1.3.3 Démarrage PXE

Certaines informations techniques de base, ainsi que les spécifications PXE complètes, sont disponibles dans la spécification de l'environnement PXE (Preboot Execution Environment), à l'adresse ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf.

1 Accédez au répertoire du référentiel de l'installation, et copiez les fichiers `linux`, `initrd`, `message` et `memtest` dans le répertoire `/srv/tftpboot` en entrant la commande suivante :

```
cp -a boot/loader/linux boot/loader/initrd
 boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Installez le paquetage `syslinux` directement à partir de vos CD ou DVD d'installation, à l'aide de YaST.

3 Copiez le fichier `/usr/share/syslinux/pxelinux.0` vers le répertoire `/srv/tftpboot` en entrant la commande suivante :

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Accédez au répertoire du référentiel de l'installation et copiez le fichier `isolinux.cfg` vers `/srv/tftpboot/pxelinux.cfg/default` en exécutant la commande suivante :

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

5 Modifiez le fichier `/srv/tftpboot/pxelinux.cfg/default` et supprimez les lignes commençant par `gfxboot`, `readinfo` et `framebuffer`.

6 Insérez les entrées suivantes sur les lignes d'ajout des libellés `failsafe` et `apic` par défaut :

`insmod=e100`
Cette entrée permet de charger le module de kernel d'une carte réseau Intel 100 Mbits/s sur les clients PXE. Elle dépend du matériel du client et doit être adaptée en conséquence. Dans le cas d'une carte réseau Broadcom GigaBit, utilisez l'entrée suivante : `insmod=bcm5700`.

`netdevice=eth0`

Cette entrée définit l'interface réseau du client à utiliser pour l'installation du réseau. Elle n'est nécessaire que si le client est équipé de plusieurs cartes réseau et elle doit être adaptée en conséquence. Dans le cas d'une carte réseau unique, vous pouvez omettre cette entrée.

`install=nfs://`*`ip_serveurinst`*`/`*`chemin_sourceinst`*`/CD1`

Cette entrée définit le serveur NFS et la source de l'installation client. Remplacez la variable *`ip_serveurinst`* par l'adresse IP réelle du serveur d'installation. *`chemin_sourceinst`* correspond au chemin réel des sources d'installation. Les sources HTTP, FTP ou SMB sont désignées de manière semblable, à l'exception du préfixe de protocole, qui doit être ici `http`, `ftp` ou `smb`.

IMPORTANT

Si vous devez transmettre d'autres options de démarrage aux routines d'installation, telles que des paramètres de démarrage SSH ou VNC, ajoutez-les dans l'entrée `install`. Pour obtenir une présentation des paramètres, accompagnée de quelques exemples, consultez la Section 1.4, « Démarrage du système cible pour l'installation » (p. 52).

Retrouvez ci-dessous un exemple de fichier `/srv/tftpboot/pxelinux.cfg/default`. Ajustez le préfixe de protocole pour que la source d'installation corresponde à votre configuration réseau ; indiquez ensuite votre méthode préférée de connexion au programme d'installation en ajoutant à l'entrée `install` les options `vnc` et `vncpassword`, ou`ssh` et `sshpassword`. Les lignes séparées par une barre oblique inversée (\) doivent être entrées sous forme de ligne continue, sans saut de ligne ni barre oblique inversée (\).

```
default linux

# libellé par défaut
linux
 kernel linux
  append initrd=initrd ramdisk_size=65536 insmod=e100 \
  install=nfs://ip_instserver/chemin_sourceinst/produit

# libellé de type failsafe
failsafe
 kernel linux
 append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
```

```
 insmod=e100 install=nfs://ip_serveurinst/chemin_sourceinst/produit

# libellé de type apic
apic
 kernel linux
 append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
 install=nfs://ip_serveurinst/chemin_sourceinst/produit

# libellé manuel
manual
 kernel linux
 append initrd=initrd ramdisk_size=65536 manual=1

# libellé de secours
rescue
 kernel linux
 append initrd=initrd ramdisk_size=65536 rescue=1

# libellé de test mémoire
memtest
 kernel memtest

# libellé de disque dur
harddisk
 kernel linux
 append SLX=0x202

implicit     0
display      message
prompt       1
timeout      100
```

Remplacez `ip_serveurinst` et `chemin_sourceinst` par les valeurs utilisées dans votre configuration.

La section suivante offre une brève référence aux options PXELINUX utilisées dans cette configuration. Pour plus d'informations sur les options disponibles, consultez la documentation du paquetage `syslinux`, située sous `/usr/share/doc/packages/syslinux/`.

1.3.4 Options de configuration PXELINUX

Les options répertoriées ici constituent un sous-ensemble de toutes les options disponibles pour le fichier de configuration PXELINUX.

DEFAULT *options kernel...*

Définit la ligne de commande de kernel par défaut. Si PXELINUX démarre automatiquement, il agit comme si les entrées qui figurent après DEFAULT avaient été saisies à l'invite de démarrage, et ce à une exception près : l'option auto est ajoutée automatiquement, ce qui indique un démarrage automatique.

Si aucun fichier de configuration n'existe ou si l'entrée DEFAULT n'apparaît pas dans le fichier de configuration, la valeur par défaut est le nom de kernel « linux », sans autres options.

APPEND *options...*

Ajoute une ou plusieurs options à la ligne de commande du kernel. Celles-ci sont ajoutées pour les démarrages automatique et manuel. Les options sont ajoutées en tout début de ligne de commande du kernel ; en règle générale, elles peuvent être remplacées par les options de kernel entrées de manière explicite.

LABEL *libellé* KERNEL *image* APPEND *options...*

Indique que si le *libellé* est entré comme étant le kernel à démarrer, PXELINUX doit démarrer à la place l'*image*, et les options d'ajout APPEND spécifiées doivent être utilisées à la place de celles spécifiées dans la section principale du fichier (avant la première commande LABEL). La valeur par défaut de la variable *image* est identique à celle de *libellé* ; si aucune option APPEND n'est fournie, l'entrée globale (le cas échéant) est utilisée par défaut. Vous pouvez utiliser jusqu'à 128 entrées LABEL.

GRUB utilise la syntaxe suivante :

```
title mytitle
 kernel mon_kernelmes_options_kernel
 initrd mon_initrd
```

tandis que PXELINUX utilise la syntaxe ci-dessous :

```
label monlibellé
 kernel monkernel
 append mesoptions
```

Les libellés sont tronqués comme s'il s'agissait de noms de fichier et ils doivent être uniques après cette opération. Par exemple, les deux libellés « v2.1.30 » et « v2.1.31 » ne pourraient pas être différenciés sous PXELINUX car, une fois tronqués, ils portent tous deux le même nom de fichier DOS.

Il n'est pas impératif d'utiliser un kernel Linux ; vous pouvez avoir recours à un secteur d'amorçage ou un fichier COMBOOT.

APPEND -

N'ajoute rien. Vous pouvez utiliser l'option `APPEND` suivie d'un seul trait d'union comme argument dans une section `LABEL` pour remplacer une option `APPEND` globale.

`LOCALBOOT` ***`type`***

Sous PXELINUX, si vous remplacez une option `KERNEL` par `LOCALBOOT 0`, vous appelez ce libellé précis, et entraînez le démarrage du disque local et non du kernel.

Argument	Description
0	Effectue un démarrage normal.
4	Effectue un démarrage local avec le pilote UNDI (Universal Network Driver Interface - Interface de pilote réseau universelle) qui réside toujours en mémoire.
5	Effectue un démarrage local avec l'intégralité de la pile PXE, y compris le pilote UNDI, qui réside toujours en mémoire.

Aucune autre valeur n'est définie. Si vous ne savez pas à quoi correspondent les piles UNDI et PXE, indiquez `0`.

`TIMEOUT` ***`timeout`***

Indique la durée d'attente (en 1/10e de seconde) dans l'invite de démarrage, avant que le démarrage automatique soit lancé. Le timeout est annulé dès que l'utilisateur commence à saisir des données ; le système considère que l'utilisateur termine la commande initiée. Un timeout de zéro désactive entièrement le timeout (il s'agit également de la valeur par défaut).

La valeur maximale de timeout est 35 996 (un peu moins d'une heure).

`PROMPT` ***`val_drapeau`***

Si l'option `val_drapeau` a pour valeur 0, cet argument affiche l'invite de démarrage uniquement si vous appuyez sur les touches Shift ou Alt, ou si vous définissez les touches Verr. Maj. ou Défil (option par défaut). Si `val_drapeau` a la valeur 1, cet argument affiche toujours l'invite de démarrage.

```
F2  nomfichier
F1  nomfichier
..etc...
F9  nomfichier
F10nomfichier
```

Affiche le fichier indiqué à l'écran lorsque vous appuyez sur une touche de fonction à l'invite de démarrage. Cette option peut être utilisée pour implémenter l'aide en ligne sur le pré-lancement (normalement pour les options de ligne de commande du kernel). Afin d'assurer une compatibilité avec les versions antérieures, vous pouvez également utiliser la touche F10 à la place de F0. Il n'y a actuellement aucun moyen de lier les noms de fichier aux touches F11 et F12.

1.3.5 Préparation du système cible pour le démarrage PXE

Préparez le BIOS du système pour le démarrage de l'environnement PXE en incluant l'option PXE dans l'ordre de démarrage du BIOS.

AVERTISSEMENT

Ne placez pas l'option PXE avant l'option de démarrage du disque dur dans le BIOS. Le système essaierait sinon de se réinstaller chaque fois que vous le démarrez.

1.3.6 Préparation du système cible pour la fonction Wake on LAN (réveil à distance)

Pour la fonction Wake on LAN (WOL), vous devez activer l'option BIOS appropriée avant d'effectuer l'installation. Notez également l'adresse MAC du système cible. Ces informations sont nécessaires pour lancer la fonction Wake on LAN.

1.3.7 Wake on LAN (réveil à distance)

La fonction Wake on LAN permet à une machine d'être alimentée via l'envoi d'un paquet réseau spécial qui contient l'adresse MAC de la machine. Comme chaque machine au monde dispose d'un identificateur MAC unique, vous ne risquez pas de mettre par erreur la mauvaise machine sous tension.

IMPORTANT

Si la machine de contrôle n'est pas située sur le même segment réseau que la cible d'installation à réveiller, vous devez configurer les requêtes WOL afin qu'elles soient envoyées en mode multidiffusion ou contrôler à distance une machine de ce segment réseau afin qu'il joue le rôle de l'expéditeur de ces requêtes.

1.3.8 Fonction Wake on LAN (réveil à distance) manuelle

1. Loguez-vous en tant qu'utilisateur root.

2. Sélectionnez *YaST* → *Installer et supprimer des logiciels*, puis installez le paquetage `netdiag`.

3 Ouvrez une fenêtre de terminal et entrez la commande suivante en tant qu'utilisateur root pour réveiller la cible :

```
ether-wakemac_cible
```

Remplacez `mac_cible` par l'adresse MAC réelle de la cible.

1.4 Démarrage du système cible pour l'installation

Il existe deux manières différentes de personnaliser le processus de démarrage pour l'installation, en plus de celles exposées dans la Section 1.3.7, « Wake on LAN (réveil à distance) » (p. 51) et Section 1.3.3, « Démarrage PXE » (p. 45). Vous pouvez utiliser les options de démarrage par défaut et les touches de fonction (F), ou vous servir de l'invite de saisie des options de démarrage fournie dans l'écran de démarrage de l'installation, afin de transmettre les options correspondantes dont le kernel d'installation peut avoir besoin pour ce matériel particulier.

1.4.1 Utilisation des options de démarrage par défaut

Les options de démarrage ont déjà été décrites en détail dans la Chapitre *Installation avec YaST* (↑Démarrage).

Il suffit généralement de sélectionner *Installation* pour démarrer le processus de démarrage de l'installation. En cas de problème, l'option *Installation - ACPI désactivé* ou *Installation - Paramètres sécurisés* peut s'avérer utile.

Pour plus d'informations sur le dépannage du processus d'installation, consultez la Section « Problèmes d'installation » (Chapitre 9, *Problèmes courants et solutions associées*, ↑Démarrage).

1.4.2 Utilisation des touches de fonction (F)

La barre de menu située au bas de l'écran propose certaines fonctionnalités avancées indispensables dans certaines configurations. À l'aide des touches de fonction (F), vous pouvez indiquer des options supplémentaires à transmettre aux routines d'installation ; vous n'avez, pour cela, pas besoin de connaître la syntaxe précise de ces paramètres (ce qui n'est pas le cas si vous les entrez comme options de démarrage) (voir Section 1.4.3, « Utilisation des options de démarrage personnalisées » (p. 54)).

Le tableau ci-dessous dresse la liste complète des options disponibles.

***Tableau 1.1** Touches de fonction (F) au cours de l'installation*

Touche	Fonction	Options disponibles	Valeur par défaut
F1	Affichage de l'aide	Aucune	Aucune
F2	Sélection de la langue d'installation	Toutes les langues prises en charge	Anglais
F3	Modification de la résolution de l'écran pour l'installation	• Mode texte • VESA • résolution n° 1 • résolution n° 2 • ...	• La valeur par défaut dépend de votre carte graphique
F4	Sélection de la source d'installation	• CD-ROM/DVD • SLP	CD-ROM/DVD

Touche	Fonction	Options disponibles	Valeur par défaut
		• FTP • HTTP • NFS • SMB • Disque dur	
F5	Application du disque de mise à jour des pilotes	Lecteur	Aucune

1.4.3 Utilisation des options de démarrage personnalisées

L'utilisation de l'ensemble approprié d'options de démarrage facilite la procédure d'installation. De nombreux paramètres peuvent également être configurés ultérieurement à l'aide des routines linuxrc, mais l'utilisation des options de démarrage s'avère plus simple. Dans certaines configurations automatisées, les options de démarrage peuvent être fournies par `initrd` ou un fichier `info`.

Le tableau suivant répertorie tous les scénarios d'installation mentionnés dans ce chapitre, et indique les paramètres requis pour le démarrage et les options associées. Il vous suffit de toutes les ajouter dans l'ordre dans lequel elles apparaissent dans ce tableau pour obtenir une chaîne d'options de démarrage à transmettre aux routines d'installation. Par exemple (toutes sur une seule ligne) :

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Remplacez toutes les valeurs (...) de cette chaîne par les valeurs adaptées à votre configuration.

Tableau 1.2 Scénarios d'installation (démarrage) utilisés dans ce chapitre

Scénario d'installation	Paramètres nécessaires pour le démarrage	Options de démarrage
Chapitre *Installation avec YaST* (↑Démarrage)	Aucune : le système démarre automatiquement	Aucune n'est nécessaire
Section 1.1.1, « Installation à distance simple via VNC : configuration réseau statique » (p. 22)	• Emplacement du serveur d'installation • Périphérique réseau • Adresse IP • Masque de réseau • Passerelle • Fonctionnalité VNC • Mot de passe VNC	• install=(nfs,http,?ftp,smb)://*chemin_supportinst* • netdevice=*un_périphérique_réseau* (nécessaire uniquement si plusieurs périphériques réseau sont disponibles) • hostip=*une_adresse_ip* • netmask=*un_masque_réseau* • gateway=*passerelle_ip* • vnc=1 • vncpassword=*un_motdepasse*
Section 1.1.2, « Installation à distance simple via VNC : configuration réseau dynamique via DHCP » (p. 23)	• Emplacement du serveur d'installation • Fonctionnalité VNC • Mot de passe VNC	• install=(nfs,http,?ftp,smb)://*chemin_supportinst* • vnc=1 • vncpassword=*un_motdepasse*

Scénario d'installation	Paramètres nécessaires pour le démarrage	Options de démarrage
Section 1.1.3, « Installation à distance via VNC : démarrage PXE et fonction Wake on LAN (réveil à distance) » (p. 25)	• Emplacement du serveur d'installation • Emplacement du serveur TFTP • Fonctionnalité VNC • Mot de passe VNC	Ne s'applique pas ; processus géré par PXE et DHCP
Section 1.1.4, « Installation à distance simple via SSH : configuration réseau statique » (p. 26)	• Emplacement du serveur d'installation • Périphérique réseau • Adresse IP • Masque de réseau • Passerelle • Fonctionnalité SSH • Mot de passe SSH	• install=(nfs,http,?ftp,smb)://*chemin_supportinst* • netdevice=*un_périphérique_réseau* (nécessaire uniquement si plusieurs périphériques réseau sont disponibles) • hostip=*une_adresse_ip* • netmask=*un_masque_réseau* • gateway=*passerelle_ip* • usessh=1 • sshpassword=*un_motdepasse*
Section 1.1.5, « Installation à distance simple via SSH : configuration réseau dynamique via DHCP » (p. 28)	• Emplacement du serveur d'installation • Fonctionnalité SSH • Mot de passe SSH	• install=(nfs,http,?ftp,smb)://*chemin_supportinst* • usessh=1 • sshpassword=*un_motdepasse*

Scénario d'installation	Paramètres nécessaires pour le démarrage	Options de démarrage
Section 1.1.6, « Installation à distance via SSH : démarrage PXE et fonction Wake on LAN (réveil à distance) » (p. 29)	• Emplacement du serveur d'installation • Emplacement du serveur TFTP • Fonctionnalité SSH • Mot de passe SSH	Ne s'applique pas ; processus géré par PXE et DHCP

ASTUCE

Pour plus d'informations sur les options de démarrage linuxrc utilisées pour démarrer un système Linux, consultez le fichier `/usr/share/doc/packages/linuxrc/linuxrc.html`.

1.5 Surveillance du processus d'installation

Vous disposez de plusieurs options pour surveiller à distance le processus d'installation. Si vous avez indiqué les options de démarrage correctes lors du démarrage de l'installation, vous pouvez utiliser VNC ou SSH pour contrôler l'installation et la configuration du système à partir d'un poste de travail distant.

1.5.1 Installation VNC

À l'aide d'un logiciel de visualisation VNC, vous pouvez contrôler à distance l'installation de SUSE Linux à partir de presque n'importe quel système d'exploitation. Cette section vous explique comment effectuer une configuration à l'aide d'une application de visualisation VNC ou d'un navigateur Web.

Préparation de l'installation VNC

Pour préparer une installation VNC, il vous suffit de fournir, sur la cible d'installation, les options de démarrage appropriées lors du démarrage initial de l'installation (voir Section 1.4.3, « Utilisation des options de démarrage personnalisées » (p. 54)). Le système cible démarre dans un environnement texte et attend qu'un client VNC se connecte au programme d'installation.

Le programme d'installation annonce l'adresse IP et le numéro d'affichage nécessaires à l'établissement d'une connexion pour l'installation. Si vous disposez d'un accès physique au système cible, ces informations sont fournies juste après le démarrage du système en vue de l'installation. Entrez ces informations à l'invite du logiciel client VNC et fournissez votre mot de passe VNC.

La cible d'installation s'annonçant via OpenSPL, vous pouvez récupérer les informations relatives à l'adresse de la cible d'installation par le biais d'un navigateur SPL ; aucun contact physique avec l'installation n'est alors nécessaire, dans la mesure où votre configuration réseau et toutes les machines qui y figurent prennent en charge OpenSPL :

1. Lancez le fichier KDE et le navigateur Web Konqueror.

2. Entrez `service://yast.installation.suse` dans la barre d'adresse.

   Le système cible apparaît alors sous forme d'icône dans l'écran de Konqueror. Cliquez sur cette icône pour lancer la visionneuse VNC KDE dans laquelle effectuer l'installation. Vous pouvez également exécuter le logiciel de visualisation VNC en entrant l'adresse IP fournie, à la fin de laquelle vous ajoutez `:1`, pour afficher la machine sur laquelle s'effectue l'installation.

Connexion au programme d'installation

Il existe globalement deux manières de se connecter à un serveur VNC (la cible d'installation dans le cas présent). Vous pouvez démarrer une application de visualisation VNC distincte sur n'importe quel système d'exploitation ou vous connecter à l'aide d'un navigateur Web Java.

À l'aide de VNC, vous pouvez contrôler l'installation d'un système Linux à partir de tout autre système d'exploitation (notamment d'autres versions de Linux, Windows ou Mac OS).

Sur une machine Linux, assurez-vous que le paquetage tightvnc est installé. Sur une machine Windows, installez le port Windows de cette application ; il est disponible sur la page d'accueil de TightVNC (http://www.tightvnc.com/download.html).

Pour vous connecter au programme d'installation qui s'exécute sur la machine cible, procédez comme suit :

1 Démarrez la visionneuse VNC.

2 Entrez l'adresse IP et le numéro d'affichage de la cible d'installation, tels qu'ils sont fournis par le navigateur SLP ou le programme d'installation :

```
adresse_ip:numéro_affichage
```

Une fenêtre apparaît sur votre bureau ; elle affiche les écrans YaST de la même manière que pour une installation locale standard.

Lorsque vous utilisez un navigateur Web pour vous connecter au programme d'installation, vous n'avez plus besoin d'un logiciel VNC ou du système d'exploitation sous-jacent. Tant que l'application du navigateur prend en charge la fonctionnalité Java, vous pouvez utiliser n'importe quel navigateur (Firefox, Internet Explorer, Konqueror, Opera, etc.) pour effectuer l'installation de votre système Linux.

Pour effectuer une installation VNC, procédez comme suit :

1 Lancez le navigateur Web souhaité.

2 Entrez la ligne suivante à l'invite de saisie d'adresse :

```
http://adresse_ip_cible:5801
```

3 Entrez votre mot de passe VNC lorsque vous y êtes invité. La fenêtre du navigateur affiche à présent les écrans YaST, comme pour une installation locale standard.

1.5.2 Installation SSH

Grâce à SSH, vous pouvez contrôler à distance l'installation de votre machine Linux à l'aide du logiciel client SSH.

Préparation de l'installation SSH

Hormis l'installation du paquetage logiciel approprié (OpenSSH pour Linux et PuTTY pour Windows), il vous suffit de transmettre les options de démarrage correspondantes afin d'activer SSH pour l'installation. Pour plus de détails, consultez la Section 1.4.3, « Utilisation des options de démarrage personnalisées » (p. 54). OpenSSH est installé par défaut sur tout système d'exploitation SUSE Linux.

Connexion au programme d'installation

1 Récupérez l'adresse IP de la cible d'installation.

   Si vous disposez d'un accès physique à la machine cible, il vous suffit d'utiliser l'adresse IP que les routines d'installation fournissent à la console après le démarrage initial. Prenez sinon l'adresse IP qui a été attribuée à cet hôte précis lors de la configuration du serveur DHCP.

2 Sur la ligne de commande, entrez la commande suivante :

   ```
   ssh -X root@adresse_ip_cible
   ```

   Remplacez `adresse_ip_cible` par l'adresse IP réelle de la cible d'installation.

3 Lorsque vous êtes invité à saisir un nom d'utilisateur, entrez `root`.

4 Lorsque vous y êtes invité, entrez le mot de passe qui a été défini par l'intermédiaire de l'option de démarrage SSH.

   Une fois l'authentification réussie, une invite de ligne de commande pour la cible d'installation apparaît.

5 Entrez `yast` pour lancer le programme d'installation.

   Une fenêtre apparaît ; elle affiche les écrans YaSt standard, tels qu'ils sont décrits dans le Chapitre *Installation avec YaST* (↑Démarrage) .

Configuration avancée des disques 2

Les configurations système élaborées nécessitent de configurer les disques d'une certaine manière. Pour obtenir une dénomination persistante des périphériques SCSI, utilisez un script de démarrage spécifique. Conçu pour être bien plus flexible que le partitionnement physique utilisé dans les configurations standard, le modèle LVM (Logical Volume Management - Gestion des volumes logiques) est un modèle de partition de disque. Sa fonctionnalité d'instantané vous permet de créer facilement des sauvegardes de données. Le réseau RAID (Redundant Array of Independent Disks - Réseau redondant de disques indépendants) offre une intégrité, des performances et une tolérance aux pannes accrues des données.

2.1 Noms de périphérique permanents pour les périphériques SCSI

Les périphériques SCSI reçoivent lors de l'amorçage des noms de fichiers de périphérique qui leur sont attribués de manière plus ou moins dynamique. Ceci n'est pas un problème tant que ni le nombre ni la configuration des périphériques ne sont modifiés. Mais lorsque l'on ajoute un disque dur SCSI supplémentaire, et que celui-ci est reconnu par le noyau avant l'ancien disque dur, ce dernier reçoit un nouveau nom et la déclaration dans la table de montage `/etc/fstab` ne correspond plus.

Pour contourner cette difficulté, il est possible d'utiliser le script d'amorçage du système `boot.scsidev`. Activez ce script à l'aide de la commande `/sbin/insserv` et

réglez les paramètres nécessaires dans /etc/sysconfig/scsidev. Le script /etc/rc.d/boot.scsidev assure la configuration des périphériques SCSI au cours de la procédure d'amorçage et inscrit des noms de périphériques permanents dans /dev/scsi/. Ces noms de périphériques peuvent ensuite être utilisés dans /etc/fstab . De plus, il est possible de définir des noms de périphériques persistants pour la configuration SCSI dans /etc/scsi.alias. Le schéma d'attribution de nom des périphériques dans /etc/scsi est expliqué dans man scsidev

Dans le mode expert de l'éditeur de niveaux d'exécution, il faut faire appel à boot.scsidev pour l'étape B, les liens utiles sont alors placés dans /etc/init.d/boot.d, ce qui permet de créer les noms lors de l'amorçage.

ASTUCE: Noms de périphériques et udev

boot.scsidev est également pris en charge sous SUSE Linux. Cependant, il est conseillé pour créer des noms de périphériques permanents d'utiliser udev pour créer des noms de périphériques permanents dans /dev/by-id/.

2.2 Configuration du gestionnaire de volumes logiques (LVM)

Cette section décrit brièvement les principes sous-jacents à LVM et ses fonctions de base qui le rendent utile dans de nombreuses circonstances. Vous apprendrez dans la Section 2.2.2, « Configuration du gestionnaire de volumes logiques avec YaST » (p. 65) à paramétrer LVM avec YaST.

AVERTISSEMENT

Utiliser LVM peut augmenter les risques de perdre des données. Mais les risques informatiques comprennent aussi les applications qui échouent, les pannes de courant et les commandes erronées. Sauvegardez vos données avant de mettre en place LVM ou de reconfigurer les volumes. Ne travaillez jamais sans sauvegarde.

2.2.1 Le gestionnaire de volumes logiques

Le gestionnaire de volumes logiques (LVM) permet de répartir de manière flexible la place sur le disque dur entre différents systèmes de fichiers. Il a été développé car il est parfois nécessaire de modifier la répartition de l'espace disque après que le partitionnement initial a déjà été fait pendant l'installation. Comme il est difficile de modifier des partitions sur un système en cours d'exploitation, LVM fournit une réserve virtuelle d'espace disque (groupe de volumes, en abrégé VG) dans lequel des volumes logiques (LV)sont créés en fonction des besoins. Le système d'exploitation utilise alors ces derniers plutôt que les partitions physiques. Les groupes de volumes peuvent s'étendre sur plus d'un disque de manière à ce que plusieurs disques ou parties de disque puissent constituer un seul VG. LVM présente ainsi une certaine abstraction par rapport à l'espace disque physique qui permet de modifier sa répartition d'une manière bien plus simple et sûre qu'en repartitionnant physiquement. Vous trouverez des informations sur le partitionnement physique dans la section intitulée « Types de partitions » (Chapitre 1, *Installation avec YaST*, ↑Démarrage) et dans la Section « Partitionnement » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

***Figure 2.1** LVM par rapport au partitionnement physique*

La Figure 2.1, « LVM par rapport au partitionnement physique » (p. 63) compare un partitionnement physique (à gauche) et une segmentation LVM (à droite). À gauche, un seul disque a été divisé en trois partitions physiques (PART), chacune avec un point de montage (PM) attribué de manière à ce que le système d'exploitation puisse y accéder. À droite, deux disques ont été divisés en respectivement deux et trois partitions physiques. Deux volumes LVM (VG 1 et VG 2) ont été définis. VG 1 contient deux partitions du DISQUE 1 et une du DISQUE 2. VG 2 contient les deux partitions restantes du DISQUE 2. Dans LVM, les partitions de disque physiques incorporées dans un

groupe de volume sont appelées volumes physiques (PV). Dans les groupes de volumes, quatre volumes logiques (LV 1 à LV 4) ont été définis et peuvent être utilisés par le système d'exploitation par le biais des points de montages associés. Les frontières entre les différents volumes logiques ne sont pas nécessairement alignées avec les frontières de partitions. Voir la frontière entre LV 1 et LV 2 dans cet exemple.

Fonctionnalités de LVM :

- Vous pouvez rassembler plusieurs disques durs ou partitions en un seul grand volume logique.
- Si l'espace disponible sur un volume logique (par exemple `/usr`) tire à sa fin, vous pouvez l'agrandir en le configurant de manière appropriée.
- Avec le gestionnaire de volumes logiques, vous pouvez même ajouter des disques durs ou des volumes logiques dans un système en cours d'exploitation ; la condition préalable étant qu'il faut utiliser du matériel pouvant être remplacé à chaud approprié pour ce genre d'interventions.
- On peut activer un « mode d'entrelacement » (striping mode) qui distribue le flux de données d'un volume logique sur plusieurs volumes physiques. Si ces volumes physiques se situent sur des disques différents, ceci peut améliorer les performances en lecture et en écriture de la même manière que RAID 0.
- La fonctionnalité de « snapshot » (instantané) permet, notamment sur les serveurs, de réaliser des sauvegardes cohérentes alors même que le système est en cours de fonctionnement.

Ces fonctionnalités rendent déjà l'utilisation de LVM pertinente pour des ordinateurs domestiques très utilisés ou pour des petits serveurs. Si vous avez un volume de données en évolution constante comme des bases de données, des archives de musique ou des répertoires utilisateur, LVM est exactement ce qu'il vous faut. Ceci vos permet d'avoir des systèmes de fichiers plus grands que le disque dur physique. Un autre avantage de LVM est que vous pouvez créer jusque 256 volumes logiques. Gardez cependant à l'esprit que le travail avec LVM est différent du travail avec des partitions classiques. Vous trouverez des instructions et des informations supplémentaires sur la configuration des LVM dans le guide pratique officiel de LVM à l'adresse http://www.traduc.org/docs/HOWTO/lecture/LVM-HOWTO.html

À partir de la version 2.6 du noyau, la version 2 de LVM est disponible. Elle assure la compatibilité descendante avec la version précédente de LVM et peut toujours gérer

les anciens groupes de volumes. Lorsque vous créez de nouveaux groupes de volumes, vous devez décider si vous voulez utiliser le nouveau format ou la version avec compatibilité descendante. LVM 2 ne nécessite aucun correctif du noyau. Il utilise la mise en correspondance des périphériques (device mapper) intégrée au noyau 2.6. Ce noyau ne prend en charge que la version 2 de LVM. C'est pourquoi lorsque nous parlerons de LVM dans cette section nous nous référerons toujours à LVM dans sa version 2.

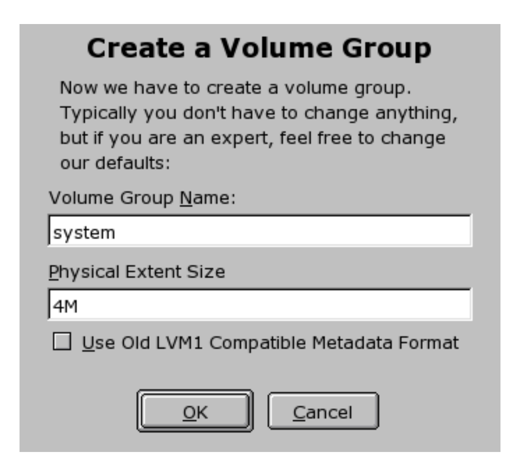
2.2.2 Configuration du gestionnaire de volumes logiques avec YaST

Vous pouvez accéder à la configuration de LVM avec YaST par le biais du partitionnement en mode expert (voir la Section « Partitionnement » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage)). Cet outil de partitionnement professionnel vous permet de modifier et de supprimer les partitions existantes et d'en créer de nouvelles qui peuvent être utilisées avec LVM. Vous pouvez y créer une partition LVM en cliquant d'abord sur *Créer* → *Ne pas formater*, puis en choisissant *0x8E Linux LVM* comme identifiant de partition. Après avoir créé toutes les partitions à utiliser avec LVM, cliquez sur *LVM* pour commencer à configurer LVM.

Créer des groupes de volumes

Si aucun groupe de volumes n'existe encore sur votre système, on vous demande d'en ajouter un (voir la Figure 2.2, « Créer un groupe de volumes » (p. 66)). On peut créer des groupes supplémentaires avec *Ajouter groupe* mais un seul groupe de volumes est généralement suffisant. Le nom `system` est suggéré pour le groupe de volumes dans lequel se trouvent les fichiers système de SUSE Linux. La taille des extensions physiques définit la taille d'un bloc physique dans le groupe de volumes. Tout l'espace disque d'un groupe de volumes est géré en morceaux de cette taille. Cette valeur est normalement définie à 4 Mo et permet une taille maximale de 256 Go pour les volumes physiques et logiques. La taille des extensions physiques ne devrait être augmentée par exemple à 8, 16 ou 32 Mo si vous avez besoin de volumes plus gros que 256 Go.

Figure 2.2 *Créer un groupe de volumes*

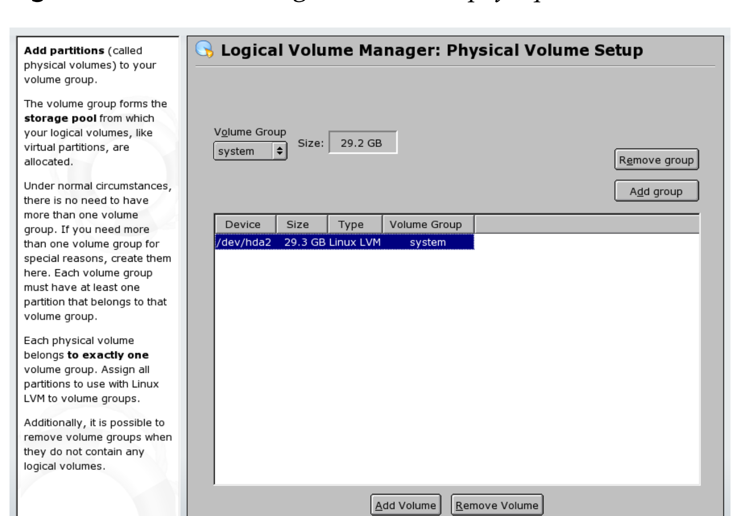


Configuration des volumes physiques

Lorsque vous avez créé un groupe de volumes, la boîtes de dialogue suivantes donnent la liste de toutes les partitions qui possèdent le type « Linux LVM » ou « Linux native ». Aucune partition d'échange ou DOS n'est affichée. Si une partition est déjà attribuée à un groupe de volumes, c'est le nom du groupe de volumes qui est affiché dans la liste. Les partitions non attribuées sont identifiées par « -- ».

Si vous utilisez plusieurs groupes de volumes, choisissez le groupe de volumes courant dans la boîte de sélection en haut à gauche. Utilisez les boutons en haut à droite pour créer des groupes de volumes supplémentaires et supprimer des groupes de volumes existants. Vous ne pouvez cependant supprimer que les groupes de volumes auxquels plus aucune partition n'est attribuée. Toutes les partitions attribuées à un groupe de volumes sont également appelées volumes physiques (Physical Volume, PV).

***Figure 2.3** Paramétrage des volumes physiques*



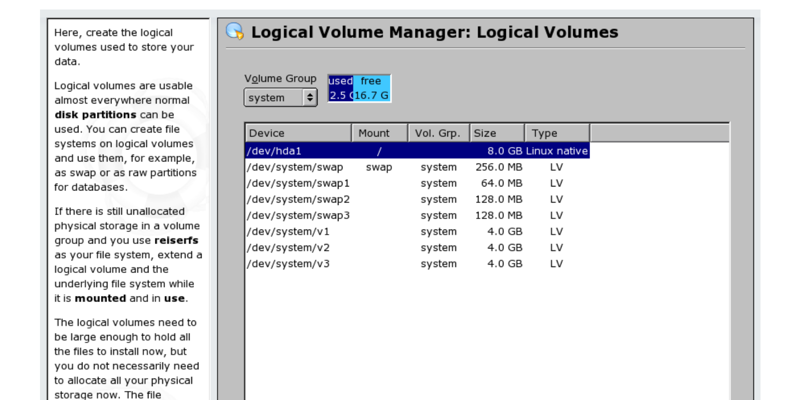
Pour ajouter dans le groupe de volumes de votre choix une partition jusqu'alors non attribuée, cliquez d'abord sur la partition, puis sur le bouton *Ajouter volume*. Le nom du groupe de volumes est alors placé à côté de la partition sélectionnée. Nous vous conseillons d'attribuer toutes les partitions que vous envisagez d'utiliser pour le gestionnaire de volumes logiques à un groupe de volumes sans quoi l'espace de la partition reste inutilisé. Avant de pouvoir quitter la boîte de dialogue, un volume physique au moins doit être attribué à chaque groupe de volumes. Après avoir attribué tous les volumes physiques, cliquez sur *Suivant* pour configurerles volumes logiques.

Configurer les volumes logiques

Une fois que le groupe de volumes a été rempli avec des volumes physiques, définissez dans la boîte de dialogue suivante les volumes logiques que le système d'exploitation doit utiliser. Choisissez le groupe de volumes courant dans la boîte de sélection en haut à gauche. L'espace disponible dans le groupe de volume courant est affiché à côté. La liste en-dessous contient tous les volumes logiques de ce groupe de volumes. Toutes les partitions Linux normales auxquelles est associé un point de montage, toutes les partitions d'échange et les volumes logiques déjà existants y sont listés. Vous pouvez *Ajouter*, *Modifier* et *Supprimer* des volumes logiques à votre convenance jusqu'à ce

que tout l'espace du groupe de volume soit utilisé. Associez au moins un volume logique à chaque groupe de volumes.

Figure 2.4 *Gestion des volumes logiques*

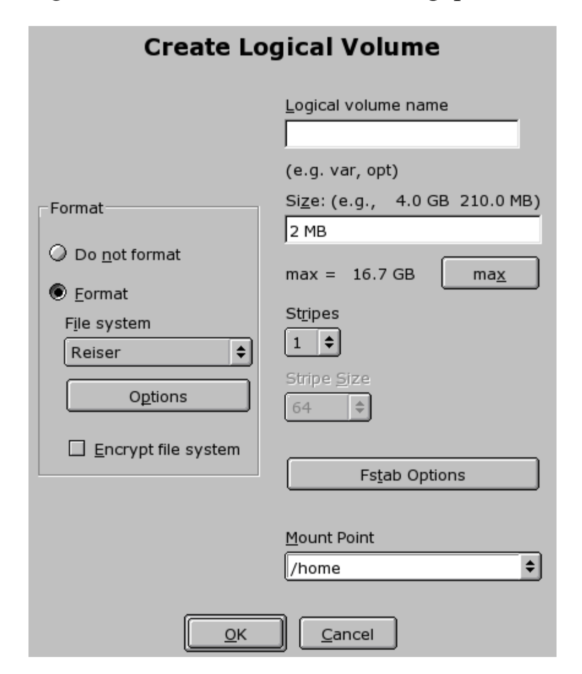


Pour créer un nouveau volume logique, cliquez sur *Ajouter* et remplissez la fenêtre qui s'ouvre. Comme pour le partitionnement, entrez la taille, le système de fichiers et le point de montage. Normalement vous créez un système de fichiers comme reiserfs ou ext2 sur le volume logique et vous lui affectez un point de montage. Les fichiers enregistrés sur ce volume logique se trouvent à ce point de montage sur le système installé. Il est de plus possible de distribuer le flux de données des volumes logiques sur plusieurs volumes physiques (entrelacement ou striping). Si ces volumes physiques se situent sur des disques durs distincts, cela implique en général de meilleurs performances en lecture et en écriture (comme en RAID 0). Cependant, un LV réparti en `n` tranches ne peut être créé correctement que si l'espace disque requis par le LV peut être distribué de manière homogène entre `n` volumes physiques. Si seuls deux volumes physiques sont disponibles, il est impossible de répartir un volume logique en trois tranches.

AVERTISSEMENT: Entrelacement

YaST n'est pas capable à ce moment de vérifier que vos déclarations concernant l'entrelacement sont correctes. Une erreur sur ce point n'apparaît que plus tard lorsque LVM est mis en place sur le disque.

Figure 2.5 *Créer des volumes logiques*



Si vous aviez déjà configuré LVM sur votre système, les volumes logiques existants apparaissent ici. Avant de continuez, associez les points de montage appropriés à ces volumes logiques. Retournez au partitionnement en mode expert de YaST avec *Suivant* et terminez-y votre travail.

Gestion directe du LVM

Si vous avez déjà configuré LVM et si vous ne voulez qu'effectuer des modifications,il existe une méthode alternative. Dans le Centre de Contrôle de YaST, choisissez *Système* → *Partitionnement*. Cette boîte de dialogue propose à peu près les actions décrites ci-dessus à l'exception du partitionnement physique. Elle montre les volumes physiques

et logiques existants dans deux listes et vous pouvez gérer votre système LVM selon les méthodes décrites précédemment.

2.3 Configuration de Soft RAID

L'objectif de la technologie RAID (Redundant Array of Independent Disks - Réseau redondant de disques indépendants) est de combiner plusieurs partitions de disque dur en un seul disque dur *virtuel*, plus volumineux, afin d'optimiser les performances, la sécurité des données ou les deux. Toutefois, l'utilisation de cette méthode n'apporte pas que des avantages. La plupart des contrôleurs RAID utilisent le protocole SCSI car il gère plus efficacement un nombre de disques durs plus important que ce que gère le protocole IDE ; de plus, SCSI est mieux adapté au traitement parallèle des commandes. Certains contrôleurs RAID prennent en charge les disques durs IDE ou SATA. Reportez-vous à la base de données de matériels, à l'adresse `http://cdb.suse.de`.

2.3.1 Soft RAID

Comme un contrôleur RAID, qui peut se révéler assez onéreux, Soft RAID est capable d'effectuer ces tâches. SUSE Linux offre la possibilité de combiner plusieurs disques dur en un seul système Soft RAID (RAID logiciel), avec l'aide de YaST : une très bonne alternative à un RAID matériel. RAID exploite plusieurs stratégies pour combiner plusieurs disques durs en un seul système RAID, chacune avec des objectifs, des caractéristiques et des avantages différents. Ces variantes sont généralement appelées *niveaux RAID*.

Les niveaux RAID courants sont les suivants :

RAID 0

Ce niveau améliore les performances de l'accès aux données, en répartissant des blocs de chaque fichier sur plusieurs disques. En fait, il ne s'agit pas vraiment d'une configuration RAID, car elle n'assure pas la sauvegarde des données, mais le nom *RAID 0*, attribué à ce système, est devenu un standard. Dans la configuration RAID 0, deux disques ou plus sont mutualisés. Les performances sont très satisfaisantes, mais, en cas de défaillance d'un seul disque dur, tout le système RAID est détruit et vos données sont perdues.

RAID 1

Ce niveau assure un degré de sécurité acceptable pour vos données, car elles sont copiées sur un autre disque, selon un système 1:1, appelé *mise en miroir de disques durs*. Si un disque est détruit, une copie de son contenu est toujours disponible sur un autre disque. Tous les disques sauf un peuvent être endommagés sans mettre vos données en danger. Les performances d'écriture sont un peu réduites dans ce processus de copie, par rapport à l'utilisation d'un accès disque unique (-10 à 20 % de rapidité). Par contre, l'accès en lecture est beaucoup plus rapide, par rapport à l'accès à un disque dur physique normal, car les données sont dupliquées et peuvent donc être consultées en parallèle. En général, le niveau 1 offre une vitesse de lecture presque deux fois supérieure à celle d'un disque unique et une vitesse d'écriture presque égale.

RAID 2 et RAID 3

Ce ne sont pas des implémentations RAID courantes. Le niveau 2 segmente les données au niveau du bit, et non du bloc. Le niveau 3 segmente les données au niveau de l'octet avec un disque de parité dédié et ne peut pas gérer plusieurs requêtes simultanées. Ces deux niveaux sont rarement utilisés.

RAID 4

Le niveau 4 segmente les données en blocs, comme le niveau 0, mais utilise un disque de parité dédié. En cas de défaillance du disque de données, les données de parité servent à créer un disque de remplacement. Cependant, le disque de parité risque de créer un goulot d'étranglement lors de l'accès en écriture. Néanmoins, le niveau 4 est parfois utilisé.

RAID 5

RAID 5 est un compromis optimisé entre le niveau 0 et le niveau 1, en ce qui concerne les performances et la redondance. L'espace disque dur équivaut au nombre de disques utilisés moins un. Les données sont réparties sur tous les disques durs, comme avec RAID 0. Des *blocs de parité* sont créés sur l'une des partitions pour assurer la sécurité. Ils sont liés les uns aux autres par l'opérateur OU exclusif (XOR) ; le contenu peut ainsi être reconstruit, avec ce même opérateur, par le bloc de parité correspondant, en cas de défaillance du système. RAID 5 ne gère pas les défaillances simultanées de plusieurs disques. Si un disque dur tombe en panne, remplacez-le dès que possible pour éviter tout risque de perte de données.

Autres niveaux RAID

D'autres niveaux RAID ont été développés (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.), dont certains dans le cadre de configurations propriétaires, créées

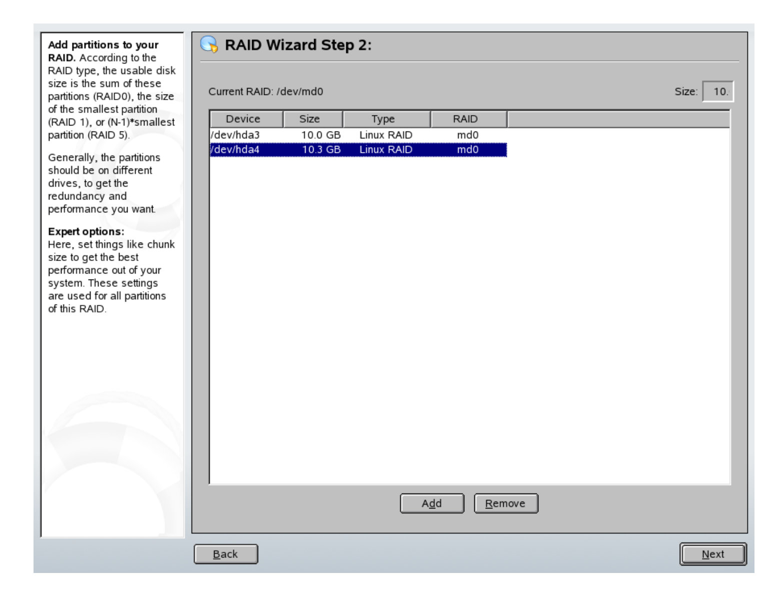
par des fabricants de matériel. Ces niveaux étant peu répandus, ils ne sont pas détaillés ici.

2.3.2 Configuration de Soft RAID avec YaST

Pour configurer Soft RAID avec YaST, vous passez par YaST Expert Partitioner, décrit à la Section « Partitionnement » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage). Cet outil de partitionnement professionnel permet de modifier et de supprimer des partitions existantes, et d'en créer d'autres pour les utiliser avec Soft RAID. Dans cet outil, vous pouvez créer des partitions RAID en cliquant d'abord sur *Créer* → *Ne pas formater*, puis en sélectionnant *0xFD Linux RAID* comme identificateur de partition. Pour RAID 0 et RAID 1, au moins deux partitions sont nécessaires ; pour RAID 1, vous devez même en avoir exactement deux, pas plus. Si vous utilisez RAID 5, vous avez besoin d'au moins trois partitions. Il est recommandé de ne choisir que des partitions de même taille. Les partitions RAID doivent être stockées sur des disques durs différents, afin de réduire le risque de perte de données si l'un des disques est défectueux (pour RAID 1 et RAID 5) et afin d'optimiser les performances (pour RAID 0). Une fois que vous avez créé toutes les partitions à utiliser avec RAID, cliquez sur *RAID* → *Créer RAID* pour démarrer la configuration de RAID.

Dans la boîte de dialogue suivante, choisissez l'un des niveaux RAID 0, RAID 1 ou RAID 5 (consultez la Section 2.3.1, « Soft RAID » (p. 70) pour plus de détails). Quand vous cliquez sur *Suivant*, la boîte de dialogue qui suit répertorie toutes les partitions de type « Linux RAID » ou « Linux natif » (consultez la Figure 2.6, « Partitions RAID » (p. 73)). Aucune partition swap ou DOS n'est affichée. Si une partition est déjà attribuée à un volume RAID, le nom du périphérique RAID (par exemple, `/dev/md0`) est affiché dans la liste. Les partitions non assignées sont indiquées par « -- ».

Figure 2.6 Partitions RAID



Pour ajouter une partition non assignée au volume RAID sélectionné, cliquez d'abord sur la partition, puis sur *Ajouter*. À ce stade, le nom du périphérique RAID est ajouté à côté de la partition sélectionnée. Assignez toutes les partitions réservées pour RAID. Sinon, l'espace de ces partitions reste inutilisé. Une fois toutes les partitions assignées, cliquez sur *Suivant* pour ouvrir la boîte de dialogue des paramètres, qui permet de régler les performances (consultez la Figure 2.7, « Paramètres du système de fichiers » (p. 74)).

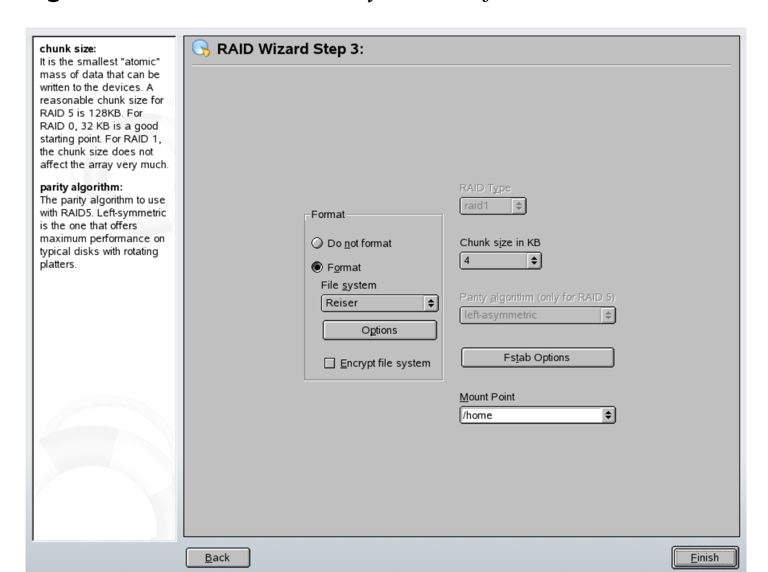


Figure 2.7 *Paramètres du système de fichiers*

Comme avec un partitionnement conventionnel, définissez le système de fichiers à utiliser, ainsi que le codage et le point de montage du volume RAID. Si vous cochez la case *Superbloc persistant*, vous garantissez que les partitions RAID sont reconnues en tant que telles au démarrage. Une fois la configuration terminée (cliquez sur *Terminer*), vous voyez le périphérique `/dev/md0`, ainsi que les autres, signalés par *RAID* dans le programme Expert Partitioner.

2.3.3 Dépannage

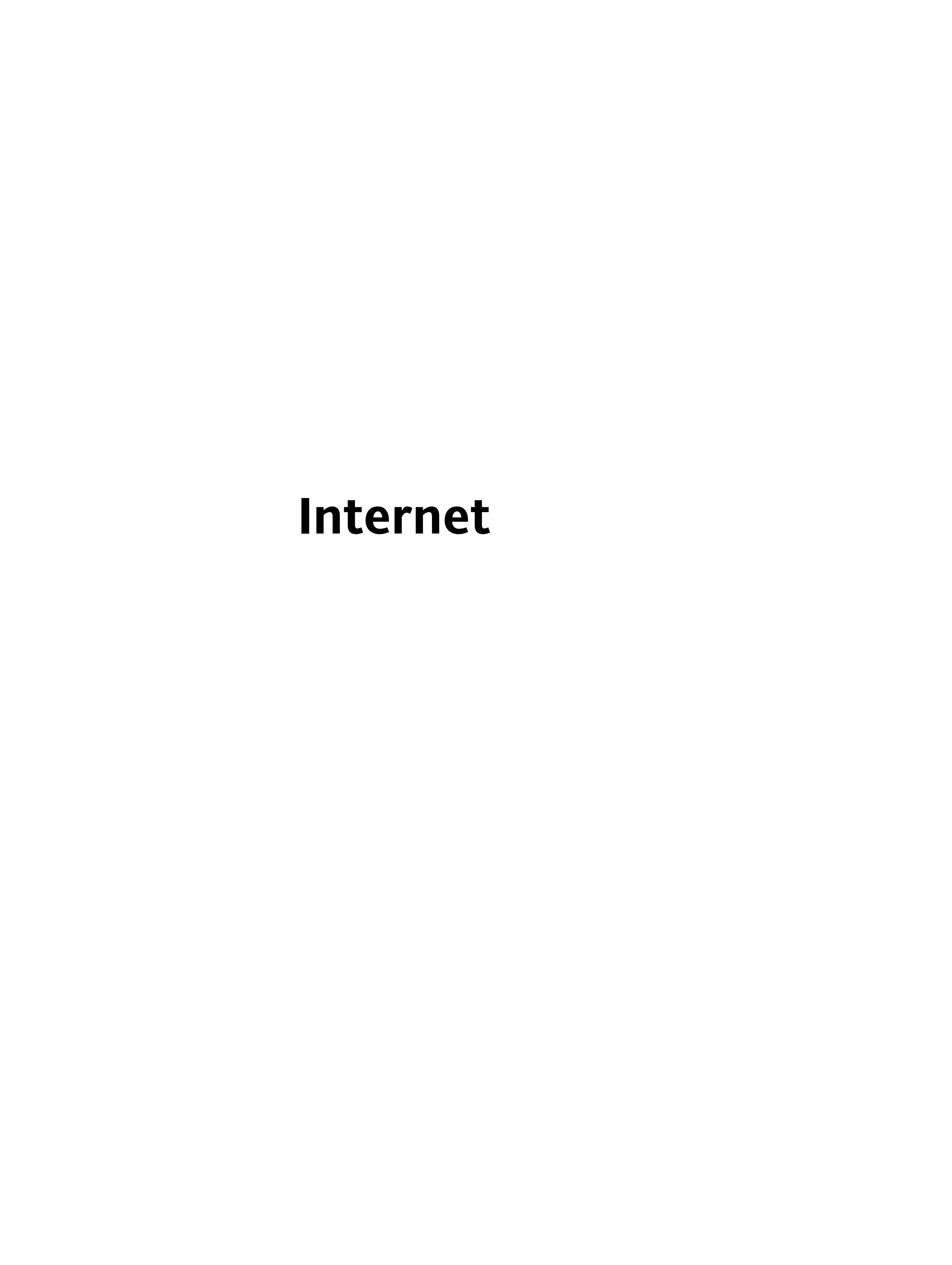
Consultez le fichier `/proc/mdstats` pour savoir si une partition RAID a été détruite. En cas de défaillance système, arrêtez votre système Linux et remplacez le disque dur défectueux par un nouveau disque partitionné de la même manière. Redémarrez ensuite votre système et entrez la commande `mdadm /dev/mdX --add /dev/sdX`. Remplacez « X » par vos identificateurs de périphérique. Cette commande intègre automatiquement le nouveau disque dur dans le système RAID et le reconstruit complètement.

2.3.4 Pour plus d'informations

Vous trouverez des instructions de configuration, ainsi que d'autres détails sur Soft RAID, dans les HOWTO (Guides pratiques), à l'adresse suivante :

- /usr/share/doc/packages/raidtools/Software-RAID.HOWTO.html
- http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html

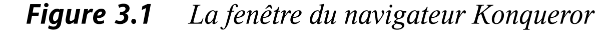
Des listes de diffusion concernant Linux RAID sont également disponibles, notamment à l'adresse http://www.mail-archive.com/linux-raid@vger.rutgers.edu.

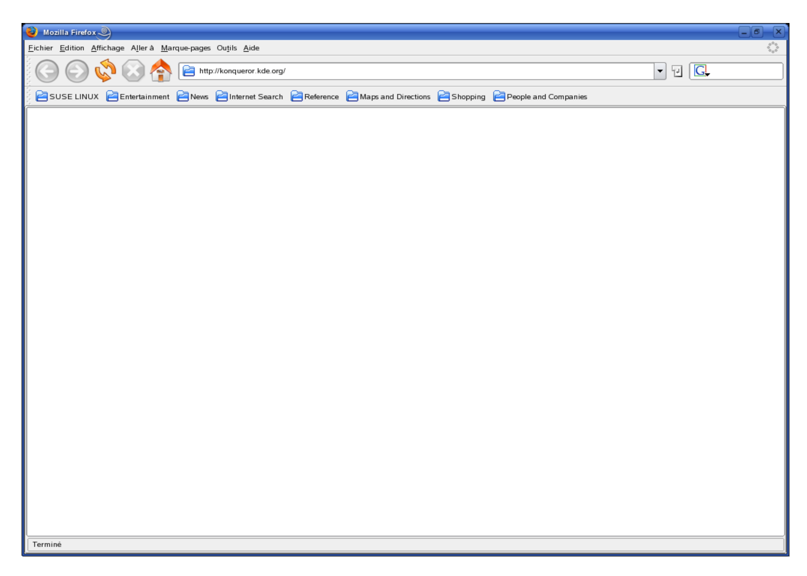

Internet

3 Le navigateur Web Konqueror

Konqueror n'est pas seulement un gestionnaire de fichiers polyvalent. C'est également un navigateur Web moderne. Si vous démarrez le navigateur en utilisant l'icône sur le panneau, Konqueror s'ouvre avec le profil de navigateur Web. Konqueror permet la navigation par onglets, la possibilité d'enregistrer des pages Web avec des images, des mots-clés Internet ou des signets, et la prise en charge de Java et de JavaScript.

Démarrez Konqueror à partir du menu principal ou en tapant la commande `konqueror`. Pour charger une page Web, entrez son adresse dans la barre d'adresses, par exemple, `http://www.suse.com`. Konqueror tente maintenant d'accéder à l'adresse et d'afficher la page. Il n'est indispensable de saisir le protocole au début de l'adresse (`http://` dans ce cas). Le programme peut compléter l'adresse automatiquement, mais ceci ne fonctionne de façon fiable qu'avec les adresses Web. Pour les adresses FTP, tapez toujours `ftp://` au début du champ de saisie.


Figure 3.1 *La fenêtre du navigateur Konqueror*



3.1 Navigation par onglets

Si vous utilisez souvent plusieurs pages Web en même temps, la navigation par onglet permet de basculer de l'une à l'autre plus facilement. Ouvrez les sites Web dans différents onglets d'une même fenêtre. L'avantage est que vous conservez un contrôle plus grand sur votre bureau du fait que vous n'avez qu'une fenêtre principale. La gestion de session KDE permet d'enregistrer votre session Web dans Konqueror à la fin de celle-ci. La prochaine fois que vous vous loguerez, Konqueror chargera les URL exactes visitées lors de la session précédente.

Pour ouvrir un nouvel onglet, sélectionnez *Fenêtre → New Tab (Nouvel onglet)* ou appuyez sur Ctrl + Shift + N. Pour changer le comportement des onglets, accédez à *Paramètres → Configure Konqueror (Configurer Konqueror)*. Dans la boîte de dialogue qui s'ouvre, sélectionnez *Comportement web → Navigation par onglets*. Pour ouvrir de nouveaux onglets plutôt que des fenêtres, activez *Open links in new tab instead of in new window (Ouvrir les liens dans des onglets plutôt que dans des fenêtres)*. Vous pouvez également masquer la barre d'onglets en sélectionnant *Hide the tab bar when only one tab is open (Masquer la barre d'onglets quand un seul onglet est ouvert)*. Pour afficher d'autres options, appuyez sur *Options avancées*.

Vous pouvez enregistrer vos onglets avec des URL et la position de la fenêtre dans un profil. Ceci est légèrement différent de la gestion de session mentionnée ci-dessus. Avec les profils, vos onglets sont à portée de main et ne requièrent pas de délai au démarrage comme avec la gestion de session.

Dans Konqueror, accédez à *Paramètres → Configure View Profiles (Configurer les profils d'affichage)* et donnez un nom à votre profil. Vous pouvez également enregistrer la taille de la fenêtre dans le profil, grâce à l'option correspondante. Vérifiez que l'option *Save URLs in profile (Enregistrer les URL dans le profil)* est sélectionnée. Cliquez sur *Enregistrer* pour confirmer. La prochaine fois que vous aurez besoin de votre « collection d'onglets », sélectionnez *Paramètres → Load View Profile (Charger le profil d'affichage)* et consultez le nom dans le menu. Lorsque vous avez sélectionné le nom, Konqueror restaure vos onglets.

3.2 Enregistrement de pages Web et de graphiques

À l'instar d'autres navigateurs, Konqueror vous permet d'enregistrer des pages Web. Pour ce faire, sélectionnez *Emplacement → Enregistrer sous* et spécifiez un nom pour votre fichier HTML. Les images ne sont toutefois pas enregistrées. Pour archiver une page Web complète, images comprises, sélectionnez *Outils → Archiver la page Web*. Konqueror suggère un nom de fichier que vous pouvez généralement accepter. Ce nom porte l'extension `.war`, qui correspond aux archives Web. Pour afficher l'archive Web enregistrée ultérieurement, cliquez simplement sur le fichier correspondant. La page Web s'affiche, avec ses images, dans Konqueror.

3.3 Mots-clés Internet

Konqueror est un moyen très simple d'effectuer des recherches sur Internet. Konqueror définit, pour vous, plus de 70 filtres de recherche, et attribue à chacun un raccourci spécifique. Pour effectuer des recherches sur un sujet particulier sur Internet, tapez le raccourci et le mot-clé en les séparant par le signe deux points. Les résultats de la recherche apparaissent ensuite sur une nouvelle page.

Pour consulter les raccourcis déjà définis, accédez à *Paramètres → Configure Konqueror (Configurer Konqueror)*. Dans la boîte de dialogue qui s'ouvre, sélectionnez *Raccourcis*

Web. Vous pouvez maintenant voir les noms des fournisseurs de recherche et les raccourcis. Konqueror définit de nombreux filtres de recherche : les moteurs de recherche « classiques », tels que Google, Yahoo et Lycos, ainsi qu'un certain nombre de filtres pour des besoins moins courants, tels qu'une base de données d'acronymes, une base de données de films Internet, ou des recherches d'applications KDE.

Si vous ne trouvez pas ici votre moteur de recherche préféré, vous pouvez facilement en définir un nouveau. Par exemple, pour rechercher certains articles intéressants dans notre base de données de support, accédez à `http://portal.suse.com/`, ouvrez la page de recherche et entrez votre requête. Ceci peut être simplifié en utilisant des raccourcis. Dans la boîte de dialogue mentionnée, sélectionnez *Nouveau* et donnez un nom à votre raccourci dans *Search provider name (Rechercher un nom de fournisseur)*. Entrez vos abréviations dans *URI shortcuts (Raccourcis URI)*. Vous pouvez en saisir plusieurs en les séparant par des virgules. La zone de texte importante est *Search URI (Recherche URI)*. Lorsque vous appuyez sur Shift + F1 et que vous cliquez sur le champ, une petite fenêtre d'aide s'ouvre. La requête de recherche est spécifiée en tant que `\{@}`. Le problème est de l'insérer au bon endroit. Dans ce cas, les paramètres de la base de données de support de SUSE ressemblent à ceci : *Search provider name (Rechercher un nom de fournisseur)* est `SUSE Support Database`, *Search URI* est (une ligne) `https://portal.suse.com/PM/page/search.pm?q=\{@}&t=optionSdbKeywords&m=25&l=en&x=true`, et *URI shortcuts (Raccourcis URI)* est `sdb_fr`.

Après avoir approuvé deux fois avec *OK*, entrez votre requête dans la barre d'adresses de Konqueror, par exemple, `sdb_fr:kernel`. Le résultat apparaît dans la fenêtre actuelle.

3.4 Signets

Plutôt que de mémoriser et de ressaisir les adresses des sites que vous visitez souvent, vous pouvez marquer les pages de ces URL à l'aide du menu *Bookmark (Signet)*. Hormis les adresses des pages Web, vous pouvez également marquer des répertoires de votre disque dur local de cette manière.

Pour créer un nouveau signet dans Konqueror, cliquez sur *Signets* → *Ajouter un signet*. Les signets ajoutés précédemment sont inclus comme des éléments dans le menu. Il est judicieux d'organiser les signets par sujets dans une structure hiérarchique, afin que vous ne perdiez pas la trace des différents éléments. Pour créer un nouveau sous-groupe

de signets, cliquez sur *New Bookmark Folder (Nouveau dossier de signets)*. Pour ouvrir l'éditeur de signets, sélectionnez *Signets → Éditer les signets*. Utilisez ce programme pour organiser, reclasser, ajouter et supprimer vos signets.

Si vous utilisez Netscape ou Mozilla ou Firefox comme navigateurs supplémentaires, il n'est pas nécessaire de recréer vos signets. L'option *Fichier → Importer les signets de Netscape* dans l'éditeur de signets vous permet d'intégrer vos signets Netscape et Mozilla dans votre dernière collection en date. L'inverse est également possible grâce à l'option *Export as Netscape Bookmark* (Exporter en tant que signet Netscape).

Pour modifier un signet, cliquez avec le bouton droit de la souris sur l'entrée correspondante. Le menu contextuel qui s'affiche vous propose plusieurs actions (couper, copier, supprimer, etc.). Une fois que vous avez atteint le résultat souhaité, enregistrez le signet en sélectionnant *Fichier → Enregistrer*. Si vous souhaitez uniquement changer le nom ou le lien, il suffit de cliquer avec le bouton droit sur l'entrée dans la barre d'outils de signet et de sélectionner *Propriétés*. Changez le nom et l'emplacement et confirmez en cliquant sur *Actualisation*.

Pour enregistrer votre liste de signets et y accéder de manière instantanée, rendez-les visibles dans Konqueror. Sélectionnez *Paramètres → Barres d'outils → Bookmark Toolbar (Konqueror) (Barre d'outils de signets Konqueror)*. Un panneau de signets est automatiquement intégré dans votre fenêtre Konqueror active.

3.5 Java et JavaScript

Java et Javascript sont deux langages à ne pas confondre. Java est un langage de programmation orienté objet, indépendant de la plate-forme utilisée, inventé par Sun Microsystems. Il est fréquemment utilisé pour créer de petits programmes (applets) exécutés au travers d'Internet par des sites d'opérations bancaires en ligne, de discussion et d'achats. JavaScript est un langage de script interprété principalement utilisé dans la structuration dynamique de pages Web, par exemple pour les menus et autres effets.

Konqueror permet d'activer ou de désactiver ces deux langages. Vous pouvez même le faire en fonction du domaine, ce qui signifie que vous pouvez autoriser l'accès à certains hôtes et le refuser à d'autres. Java et JavaScript sont souvent désactivés pour des raisons de sécurité. Malheureusement, certains pages Web ont besoin de JavaScript pour s'afficher correctement.

3.6 Pour plus d'informations

Pour toute question ou problème relatifs à l'utilisation de Konqueror, consultez le manuel de l'application, disponible dans le menu d'*Aide*. Konqueror a également une page Web, à l'adresse `http://www.konqueror.org`.

Firefox

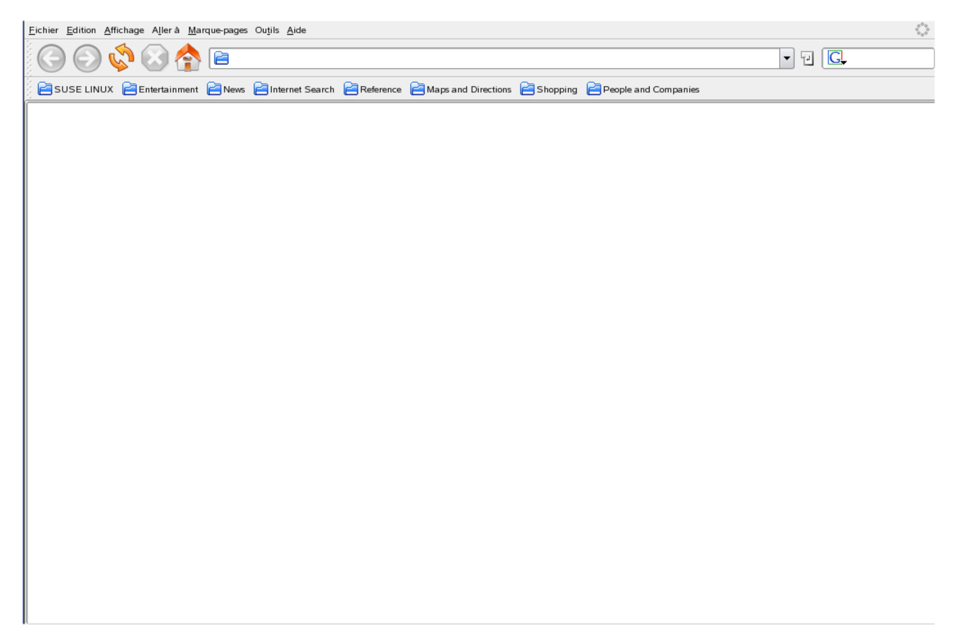
4

SUSE Linux est livré avec le navigateur Web Mozilla Firefox. Avec des fonctions telles que les onglets, le blocage des popups et la gestion des images, Firefox combine les dernières technologies Web. Il vous permet d'afficher plusieurs pages Web dans une seule fenêtre, de supprimer les publicités gênantes et de désactiver les images qui vous ralentissent. Il fournit un accès aisé à différents moteurs de recherche pour vous aider à rechercher les informations dont vous avez besoin. Pour l'ouvrir, choisissez-le dans le menu principal ou entrez la commande `firefox`. Les sections suivantes décrivent les principales fonctions du programme.

4.1 Consultation de sites Web

Firefox est similaire, en termes d'aspect et de fonctionnement, à n'importe quel autre navigateur. Il est présenté à la Figure 4.1, « La fenêtre du navigateur Firefox » (p. 86). La barre d'outils de navigation contient les boutons *Avancer d'une page* et *Reculer d'une page*, ainsi qu'une barre d'adresses Web. Les signets offrent également un accès rapide au Web. Pour plus d'informations sur les fonctions de Firefox, utilisez le menu *Aide*.


Figure 4.1 La fenêtre du navigateur Firefox



4.1.1 Navigation par onglets

Si vous utilisez souvent plusieurs pages Web en même temps, la navigation par onglet permet de basculer de l'une à l'autre plus facilement. Ouvrez les sites Web dans différents onglets d'une même fenêtre.

Pour ouvrir un nouvel onglet, sélectionnez *Fichier* → *Nouvel onglet*. Un onglet vide s'ouvre dans la fenêtre Firefox. Vous pouvez également cliquer avec le bouton droit sur un lien et sélectionner *Ouvrir dans un nouvel onglet*. Cliquez avec le bouton droit sur l'onglet lui-même pour accéder aux options qu'il contient. Vous pouvez créer un nouvel onglet, recharger un ou tous les onglets existants, ou les fermer.

4.1.2 Utilisation du panneau latéral

La partie gauche de la fenêtre du navigateur peut afficher les marque-pages ou l'historique de navigation (ou fournir encore d'autres options, avec certaines extensions).

Pour afficher le panneau latéral, choisissez *Affichage → Panneau latéral* et sélectionnez le type de contenu à afficher.

4.2 Recherche d'informations

Firefox offre deux méthodes de recherche d'informations : la barre de recherche et la barre Rechercher. La barre de recherche cherche des pages sur Internet, alors que la barre Rechercher effectue des recherches dans la page en cours.

4.2.1 Utilisation de la barre de recherche

Firefox comporte une barre de recherche qui peut accéder à différents moteurs, tels que Google, Yahoo ou Amazon. Par exemple, pour rechercher des informations concernant SUSE à l'aide du moteur en cours, cliquez sur la barre de recherche, tapez `SUSE` et appuyez sur Entrée. Le résultat apparaît dans la fenêtre. Pour choisir un moteur de recherche, cliquez sur l'icône du moteur dans la barre de recherche. Un menu s'ouvre. Il répertorie les moteurs de recherche disponibles.

4.2.2 Utilisation de la barre Rechercher

Pour effectuer une recherche à l'intérieur d'une page Web, cliquez sur *Edition → Rechercher dans la page* ou appuyez sur Ctrl + F. La barre Rechercher s'ouvre, généralement en bas de la fenêtre. Saisissez votre requête dans le champ correspondant. Firefox met en surbrillance toutes les occurrences de l'expression recherchée. L'option *Surligner* active ou désactive la mise en surbrillance.

4.3 Gestion des marque-pages

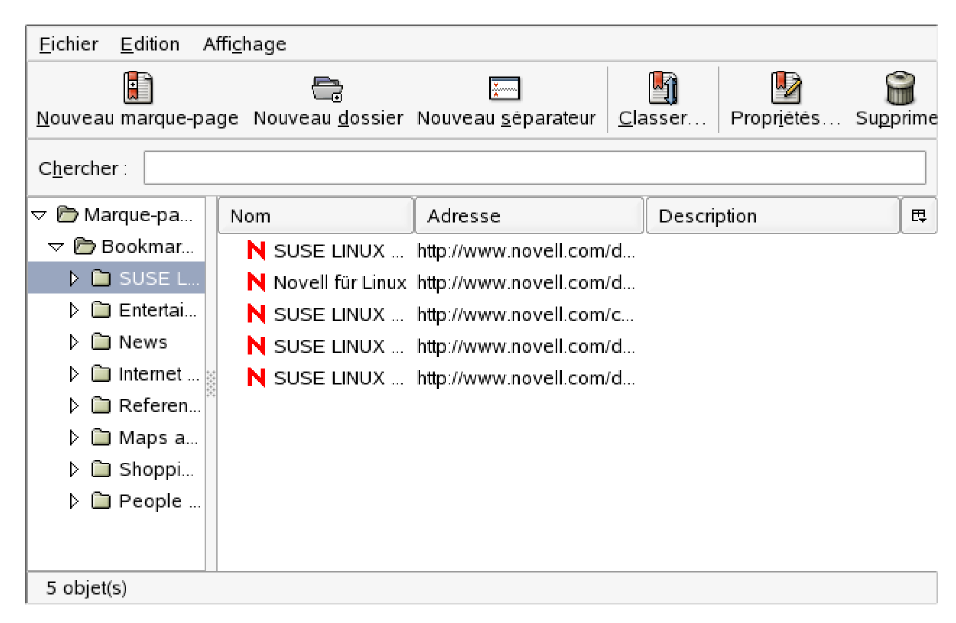
Les marque-pages sont un moyen pratique pour enregistrer des liens vers vos sites Web favoris. Pour ajouter le site Web actuel à votre liste de marque-pages, cliquez sur *Marque-pages → Marquer cette page*. Si votre navigateur affiche actuellement plusieurs sites Web dans des onglets, seule l'URL de l'onglet actuellement sélectionné est ajoutée à votre liste de marque-pages.

Lorsque vous ajoutez un marque-page, vous pouvez lui donner un autre nom et choisir le dossier où vous voulez l'enregistrer. Pour supprimer un site Web de la liste de marque-pages, cliquez sur *Marque-pages*, cliquez avec le bouton droit sur le marque-page du site dans la liste et sélectionnez *Supprimer*.

4.3.1 Utilisation du gestionnaire de marque-pages

Le gestionnaire de marque-pages vous permet de gérer les propriétés (nom et adresse) de chaque marque-page et d'organiser les marque-pages en dossiers et en sections. Il ressemble à la Figure 4.2, « Utilisation du gestionnaire de marque-pages de Firefox » (p. 88).

Figure 4.2 *Utilisation du gestionnaire de marque-pages de Firefox*



Pour ouvrir le gestionnaire de marque-pages, cliquez sur *Marque-pages → Gérer les marque-pages*. Une fenêtre affiche les marque-pages. Cliquez sur *Nouveau dossier* pour créer un nouveau dossier et lui donner un nom et une description. Si vous avez besoin d'un nouveau marque-pages, cliquez sur *Nouveau marque-page*. Une fenêtre vous permet de spécifier le nom, l'emplacement, le mot-clé et de saisir une description

du nouveau marque-page. Le mot-clé est un raccourci vers le marque-page. Si vous souhaitez afficher le marque-page que vous venez de créer dans le panneau latéral, cochez la case *Charger ce marque-page comme panneau latéral*.

4.3.2 Migration des marque-pages

Si vous utilisiez précédemment un autre navigateur, vous souhaiterez sûrement réutiliser vos préférences et vos marque-pages dans Firefox. À l'heure actuelle, Firefox permet d'importer des données de Netscape 4.x, 6, 7, Mozilla 1.x et Opera.

Pour importer des paramètres, cliquez sur *Fichier* → *Importer*. Sélectionnez le navigateur qui contient les paramètres à importer. Cliquez sur *Suivant*. Les paramètres sont importés. Les marque-pages importés sont placés dans un nouveau dossier, dont le nom commence par `Importé depuis`.

4.3.3 Marque-pages dynamiques

Les marque-pages dynamiques affichent des titres dans votre menu de marque-pages et vous tiennent au courant des dernières nouveautés. Ainsi, vous gagnez du temps, puisqu'il vous suffit de jeter un coup d'oeil sur vos sites favoris.

De nombreux sites et blogs prennent en charge ce format. Un site Web l'indique en affichant un rectangle orange contenant RSS dans l'angle inférieur droit. Cliquez dessus et choisissez *Subscribe to NAME OF THE FEED (S'abonner à NOM DU FLUX)*. Une boîte de dialogue vous permet de sélectionner le nom et l'emplacement du marque-page dynamique. Cliquez sur *Ajouter* pour confirmer.

Certains sites n'indiquent pas à Firefox qu'ils prennent en charge un nouveau flux, bien qu'ils le fassent. Pour ajouter manuellement un marque-page dynamique, vous devez connaître l'URL du flux. Procédez de la manière suivante.

Procédure 4.1 *Ajout manuel d'un marque-page dynamique*

1. Ouvrez le gestionnaire de marque-pages en cliquant sur *Marque-pages* → *Gérer les marque-pages*. Une nouvelle fenêtre s'ouvre.

2. Sélectionnez *Fichier* → *Nouveau marque-page dynamique*. Une boîte de dialogue apparaît.

3 Tapez le nom du marque-page dynamique et ajoutez l'URL, par exemple, http://www.novell.com/newsfeeds/rss/coolsolutions.xml. Firefox met à jour vos marque-pages dynamiques.

4 Fermez le gestionnaire de marque-pages.

4.4 Utilisation du gestionnaire de téléchargements

Le gestionnaire de téléchargements garde la trace des téléchargements effectués. Pour l'ouvrir, cliquez sur *Outils* → *Téléchargements*. Firefox ouvre une fenêtre qui répertorie les téléchargements. Lors du téléchargement d'un fichier, une barre de progression s'affiche avec le nom du fichier en cours. Vous pouvez interrompre le téléchargement et le reprendre plus tard si vous le souhaitez. Pour ouvrir un fichier téléchargé, cliquez sur *Ouvrir*. Pour effacer du disque un fichier téléchargé, cliquez sur *Supprimer*. Si vous avez besoin d'informations concernant le fichier, cliquez avec le bouton droit sur son nom et choisissez *Propriétés*.

Si vous souhaitez mieux contrôler le gestionnaire de téléchargements, ouvrez la fenêtre de configuration dans *Edition* → *Préférences* et cliquez sur l'onglet *Téléchargements*. Cette fenêtre vous permet de choisir le dossier dans lequel s'effectuera le téléchargement, de définir le comportement du gestionnaire et de configurer les actions à effectuer pour certains types de fichiers.

4.5 Personnalisation de Firefox

Firefox propose un grand nombre d'options de personnalisation : possibilité d'installer des extensions, de changer les thèmes et d'ajouter des mots-clés intelligents pour les recherches en ligne.

4.5.1 Extensions

Mozilla Firefox est une application multifonctions : vous pouvez télécharger et installer des compléments, appelés extensions. Par exemple, vous pouvez ajouter un nouveau

gestionnaire de téléchargements et de nouveaux mouvements de la souris. Cette caractéristique préserve la petite taille de Firefox.

Pour ajouter une extension, cliquez sur *Outils* → *Extensions*. Dans l'angle inférieur droit de la fenêtre, cliquez sur *Obtenir d'autres extensions*. La page Web de mise à jour des extensions Mozilla s'ouvre. Elle propose un certain nombre d'extensions. Cliquez sur l'extension à installer, puis sur le lien d'installation pour la télécharger et l'installer. Lorsque vous redémarrez Firefox, la nouvelle extension fonctionne. Vous pouvez également consulter les différentes extensions à l'adresse `http://update.mozilla.org/`.

Figure 4.3 *Installation des extensions Firefox*



4.5.2 Changement de thème

Si vous n'aimez pas l'aspect standard de Firefox, installez un nouveau *thème*. Les thèmes ne changent pas les fonctions du navigateur, mais uniquement son apparence. Lorsque vous installez un thème, Firefox vous demande d'abord de confirmer l'opération. Autorisez l'installation ou annulez-la. Lorsque l'installation est terminée, vous pouvez activer le nouveau thème.

1 Cliquez sur *Outils* → *Thèmes*.

2 Une boîte de dialogue apparaît. Cliquez sur *Obtenir d'autres thèmes*. Si vous avez déjà installé un thème, il apparaît dans la liste, comme l'illustre la Figure 4.4, « Installation de thèmes Firefox » (p. 92).

Figure 4.4 *Installation de thèmes Firefox*



3 Une fenêtre s'ouvre sur la page d'accueil du site Web `https://update.mozilla.org` (en anglais).

4 Choisissez un thème et cliquez sur *Install Now (Installer maintenant)*.

5 Confirmez le téléchargement et l'installation.

6 Lorsque vous avez téléchargé le thème, une boîte de dialogue vous présente des informations sur votre liste de thèmes. Activez le nouveau thème en cliquant sur *Utiliser le thème*.

7 Fermez la fenêtre et redémarrez Firefox.

Si vous avez installé un thème, vous pouvez toujours en changer sans redémarrer en cliquant sur *Outils* → *Thèmes* puis *Utiliser le thème*. Vous pouvez supprimer un thème que vous n'utilisez plus en cliquant sur *Désinstaller* dans la même boîte de dialogue.

4.5.3 Ajout de mots-clés à vos recherches en ligne

La recherche sur Internet est l'une des principales tâches principales d'un navigateur. Firefox vous permet de définir vos propres *mots-clés intelligents* : des abréviations à utiliser comme des « commandes » pour effectuer des recherches sur le Web. Par

exemple, si vous utilisez souvent Wikipedia, utilisez un mot-clé intelligent pour simplifier cette tâche :

1. Accédez à `http://en.wikipedia.org`.

2. Lorsque Firefox affiche la page Web, placez-vous dans la zone de texte de recherche. Cliquez dessus avec le bouton droit. Un menu s'ouvre. Choisissez *Ajouter un mot-clé pour cette recherche*.

3. La boîte de dialogue *Ajouter un marque-page* s'ouvre. Dans le champ *Nom*, donnez un nom à cette page Web, par exemple, *Wikipedia (en)*.

4. Dans le champ *Mot-clé*, entrez une abréviation pour cette page Web, par exemple, *wiki*.

5. Dans le champ *Créer dans*, choisissez l'emplacement de l'entrée dans votre dossier de marque-pages. Vous pouvez la placer dans *Recherches rapides*, mais n'importe quel autre niveau est également correct.

6. Cliquez sur *Ajouter* pour terminer.

Vous avez créé un nouveau mot-clé. Lorsque vous voudrez consulter Wikipedia, vous n'aurez plus besoin d'entrer l'URL complète. Il vous suffira de saisir `wiki Linux` pour consulter une entrée concernant Linux.

4.6 Impression à partir de Firefox

La boîte de dialogue *Mise en page* vous permet de configurer la façon dont Firefox imprime le contenu affiché. Cliquez sur *Fichier* → *Mise en page*, puis cliquez sur l'onglet *Format et options* pour choisir l'orientation d'impression de vos documents. Vous pouvez les redimensionner ou les ajuster automatiquement. Si vous souhaitez imprimer l'arrière-plan, sélectionnez *Imprimer le fond de page (couleurs et images)*. Cliquez sur l'onglet *Marges, en-tête et bas de page* pour ajuster les marges et pour sélectionner les données à placer dans les en-têtes et les bas de page.

Après avoir configuré vos paramètres, imprimez une page Web en cliquant sur *Fichier* → *Imprimer*. Sélectionnez l'imprimante, ou le fichier dans lequel vous voulez enregistrer la sortie. Dans *Propriétés*, définissez le format du papier, indiquez la commande d'im-

pression, choisissez noir et blanc ou couleur et déterminez les marges. Si les paramètres vous conviennent, cliquez sur *Imprimer*.

4.7 Pour plus d'informations

Pour en savoir plus sur Firefox, consultez la page d'accueil officielle à l'adresse `http://www.mozilla.org/products/firefox/`. Reportez-vous à l'aide intégrée pour obtenir plus d'informations sur certaines options ou fonctions.

Linphone—VoIP pour Linux Desktop 5

Linphone est une petite application de téléphonie sur le Web pour votre bureau Linux. Elle permet les communications téléphoniques entre deux personnes sur Internet. Aucun matériel spécial n'est nécessaire : une station de travail standard avec une carte son correctement configurée, un microphone et des haut-parleurs ou des écouteurs suffisent pour utiliser Linphone.

5.1 Configuration de Linphone

Avant de commencer à utiliser Linphone, vous devez prendre un certain nombre de décisions de base et réaliser un certain nombre de tâches de configuration. Commencez par déterminer et configurer le mode d'exécution de Linphone, déterminez le type de connexion à utiliser, puis démarrez la configuration de Linphone (*Aller* → *Préférences*) pour effectuer les réglages nécessaires.

5.1.1 Détermination du mode d'exécution de Linphone

Linphone peut s'exécuter dans deux modes différents, selon votre type de bureau et sa configuration.

Application normale

Après l'installation du logiciel Linphone, vous pouvez le démarrer via les menus d'application GNOME et KDE ou via la ligne de commande. Lorsque Linphone n'est pas en cours d'exécution, les appels entrants ne peuvent être reçus.

Panneau de configuration GNOME

Linphone peut être ajouté au tableau de bord de GNOME. Cliquez avec le bouton droit sur une zone vide du tableau de bord, sélectionnez *Ajouter au tableau de bord* puis sélectionnez Linphone. Linphone est alors ajouté de façon permanente au tableau de bord et redémarré automatiquement lors de la connexion. Tant que vous ne recevez pas d'appels entrants, il s'exécute en arrière-plan. Dès qu'un appel entrant arrive, la fenêtre principale s'ouvre et vous pouvez recevoir l'appel. Pour ouvrir la fenêtre principale et appeler quelqu'un, il suffit de cliquer sur l'icône de l'applet.

5.1.2 Détermination du type de connexion

Il existe plusieurs manières différentes d'appeler un correspondant dans Linphone. La façon dont vous appelez un correspondant et dont vous l'atteignez est déterminée par le type de connexion au réseau ou à Internet.

Linphone utilise le protocole SIP (Session Initiation Protocol) pour établir une connexion avec un hôte distant. Dans SIP, chaque partie est identifiée par une URL SIP :

```
sip:nom d'utilisateur@nom d'hôte
```

nom d'utilisateur est votre login sur votre machine Linux et *nom d'hôte* le nom de l'ordinateur que vous utilisez. Si vous utilisez un fournisseur SIP, l'URL ressemble à l'exemple suivant :

```
sip:nom d'utilisateur@serveur sip
```

nom d'utilisateur est le nom d'utilisateur choisi lors de l'inscription auprès d'un serveur SIP. *serveur sip* est l'adresse du serveur SIP de votre fournisseur SIP. Pour plus de détails sur la procédure d'inscription, consultez la Section 5.1.5, « Configuration des options SIP » (p. 99) et consultez la documentation d'inscription du fournisseur. Pour connaître la liste des fournisseurs pouvant répondre à votre besoin, consultez les pages Web indiquées à la Section 5.8, « Pour plus d'informations » (p. 106).

L'adresse URL à utiliser est déterminée par le type de connexion que vous choisissez. Si vous choisissez d'appeler un correspondant directement, sans routage supplémentaire par un fournisseur SIP, saisissez une adresse URL du premier type. Si vous choisissez

d'appeler un correspondant via un serveur SIP, saisissez une adresse URL du second type.

Appel sur le même réseau

Si vous avez l'intention d'appeler un ami ou un collègue appartenant au même réseau, il vous suffit de connaître le nom d'utilisateur ou le nom d'hôte pour créer une adresse URL SIP valide. Ceci est également vrai pour un correspondant qui souhaite vous appeler. Tant qu'il n'y a pas de pare-feu entre vous et votre correspondant, aucune configuration supplémentaire n'est nécessaire.

Appel sur des réseaux ou sur Internet (configuration d'IP statique)

Si vous êtes connecté à Internet et si vous utilisez une adresse IP statique, quiconque veut vous appeler n'a besoin que du nom d'hôte ou de l'adresse IP de votre station de travail pour créer une adresse URL SIP valide, comme décrit dans la section intitulée « Appel sur le même réseau » (p. 97). Si vous ou votre correspondant êtes situés derrière un pare-feu qui filtre le trafic entrant et sortant, ouvrez le port SIP (`5060`) et le port RTP (`7078`) sur le pare-feu pour activer le trafic Linphone sur le pare-feu.

Appel sur des réseaux ou sur Internet (configuration d'IP dynamique)

Si votre configuration IP n'est pas statique—si vous obtenez de façon dynamique une nouvelle adresse IP chaque fois que vous vous connectez à Internet—il est impossible pour un correspondant quelconque de créer une adresse URL SIP valide basée sur votre nom d'utilisateur et une adresse IP. Dans ce cas, utilisez les services offerts par un fournisseur SIP ou utilisez une configuration DynDNS pour vous assurer qu'un correspondant externe peut se connecter à la machine hôte correcte. Pour plus d'informations sur DynDNS, consultez `http://en.wikipedia.org/wiki/Dynamic_DNS`.

Appel sur des réseaux et des pare-feu

Les machines cachées derrière un pare-feu ne révèlent pas leur adresse IP sur Internet. Ainsi, elles ne peuvent être atteintes directement par quiconque tenterait d'appeler un utilisateur travaillant sur ce type de machine. Linphone prend en charge les appels à

travers les frontières des réseaux et les pare-feu en utilisant un proxy SIP ou en relayant les appels vers un fournisseur SIP. Consultez la Section 5.1.5, « Configuration des options SIP » (p. 99) pour une description détaillée des réglages nécessaires afin d'utiliser un serveur SIP externe.

5.1.3 Configuration des paramètres du réseau

La plupart des paramètres contenus dans l'onglet *Réseau* n'ont pas besoin d'être modifiés. Vous devez pouvoir appeler un premier correspondant sans les changer.

Options de parcours NAT

N'activez cette option que si vous vous trouvez dans un réseau privé derrière un pare-feu et si vous n'utilisez pas un fournisseur SIP pour acheminer vos appels. Cochez la case et entrez l'adresse IP de la machine pare-feu en notation avec des points, par exemple, `192.168.34.166`.

Propriétés RTP

Linphone utilise le protocole RTP (real-time transport protocol) pour transmettre les données audio de vos appels. Le port pour le protocole RTP est défini sur `7078` et ne doit pas être modifié, sauf si une autre de vos applications l'utilise. Le paramètre de compensation d'instabilité permet de contrôler le nombre de paquets audio mis en mémoire tampon par Linphone avant de les lire. Lorsque vous augmentez ce paramètre, vous améliorez la qualité de transmission. Plus le nombre de paquets mis en mémoire tampon est grand, plus il y a de chances pour les « retardataires » d'être lus. D'un autre côté, le fait d'augmenter le nombre de paquets mis en mémoire tampon augmente aussi la latence : la voix de votre correspondant vous parvient avec un certain retard. Lorsque vous modifiez ce paramètre, vous devez trouver le bon équilibre entre ces deux facteurs.

Autre

Si vous utilisez une combinaison de téléphonie VoIP et par ligne terrestre, vous pouvez utiliser la technologie DTMF (double tonalité multi fréquence) pour déclencher certaines actions, telles que la consultation à distance de votre messagerie vocale en appuyant sur certaines touches. Linphone prend en charge deux protocoles pour la transmission DTMF, SIP INFO et RTP rfc2833. Si vous avez besoin de la fonctionnalité DTMF dans Linphone, choisissez un fournisseur SIP qui prend en

charge l'un de ces protocoles. Pour consulter la liste complète des fournisseurs VoIP, consultez la Section 5.8, « Pour plus d'informations » (p. 106).

5.1.4 Configuration du périphérique audio

Lorsque votre carte son a été correctement détectée par Linux, Linphone l'utilise automatiquement comme périphérique audio par défaut. Laissez la valeur de *Use sound device (Utiliser un périphérique son)* telle qu'elle est. Utilisez *Recording source (Source d'enregistrement)* pour déterminer la source d'enregistrement à utiliser. Dans la plupart des cas, il s'agira d'un microphone (`micro`). Pour sélectionner une sonnerie personnalisée, utilisez *Parcourir* pour le choisir et le tester en utilisant *Listen (Écouter)*. Cliquez sur *Appliquer* pour accepter les modifications.

5.1.5 Configuration des options SIP

La boîte de dialogue *SIP* contient tous les paramètres de configuration SIP.

Port SIP
: Déterminez sur quel port l'agent utilisateur SIP doit être exécuté. Le port SIP par défaut est `5060`. Ne modifiez pas les paramètres par défaut sauf si vous savez q'une autre application ou un autre protocole a besoin de ce port.

Identité
: Quiconque veut vous appeler directement sans utiliser un proxy SIP ou un fournisseur SIP doit connaître votre adresse IP valide. Linphone crée une adresse IP valide à votre place.

Services distants
: Cette liste contient un ou plusieurs fournisseurs de services SIP auprès desquels vous avez créé un compte utilisateur. Les informations du serveur peuvent être ajoutées, modifiées ou supprimées à tout moment. Pour en savoir plus sur la procédure d'inscription, consultez Ajout d'un proxy SIP et inscription sur un serveur SIP distant (p. 100).

Informations d'authentification
: Pour vous inscrire sur un serveur SIP distant, vous devez fournir un certain nombre d'informations d'authentification, telles qu'un mot de passe et un nom d'utilisateur. Linphone stocke ces données dès que vous les fournissez. Pour effacer ces données

pour des raisons de sécurité, cliquez sur *Clear all stored authentification data (Effacer toutes les données d'authentification stockées)*.

La liste *Remote services (Services distants)* peut comporter plusieurs adresses de proxy SIP distants ou de fournisseurs de services.

Procédure 5.1 *Ajout d'un proxy SIP et inscription sur un serveur SIP distant*

1. Choisissez votre fournisseur SIP et créez un compte utilisateur.

2. Démarrez Linphone.

3. Accédez à *Aller* → *Préférences* → *SIP*.

4. Cliquez sur *Add proxy/registrar (Ajouter proxy/registre)* pour ouvrir un formulaire d'inscription.

5. Remplissez les valeurs appropriées de *Registration Period (Période d'enregistrement)*, *SIP Identity (Identité SIP)*, *SIP Proxy (Proxy SIP)* et *Route (Routage)*. Si vous travaillez derrière un pare-feu, sélectionnez toujours *Send registration (Envoyer enregistrement)* et saisissez une valeur correcte de *Registration Period (Période d'enregistrement)*. Ceci renvoie les données d'inscription d'origine après un certain temps pour garder le pare-feu ouvert sur les ports requis par Linphone. Sinon, ces ports se ferment automatiquement si le pare-feu ne reçoit plus de paquets de ce type. Le renvoi des données d'inscription est également nécessaire pour que le serveur SIP reste informé de l'état de la connexion et de l'emplacement de l'appelant. Pour *SIP identity (Identitié SIP)* saisissez l'URL SIP devant être utilisée pour les appels locaux. Pour aussi utiliser ce serveur comme proxy SIP, saisissez les mêmes données pour *SIP Proxy (Proxy SIP)*. Enfin, ajoutez un routage facultatif, le cas échéant, et cliquez sur *OK* pour quitter la boîte de dialogue.

5.1.6 Configuration des codecs audio

Linphone prend en charge plusieurs codecs pour la transmission des données vocales. Définissez votre type de connexion et choisissez vos codecs dans la liste. Les codecs ne correspondant pas à votre type de connexion sont en rouge et ne peuvent être sélectionnés.

5.2 Test de Linphone

Utilisez `sipomatic`, un petit programme de test qui peut répondre aux appels effectués à partir de Linphone, pour tester votre configuration Linphone.

***Procédure 5.2** Test d'une configuration Linphone*

1. Ouvrez un terminal.
2. Saisissez `sipomatic` à l'invite de ligne de commande.
3. Démarrez Linphone.
4. Saisissez `sip:robot@127.0.0.1:5064` comme *SIP address (Adresse SIP)*, puis cliquez sur *Call or Answer (Appeler ou répondre)*.
5. Si Linphone est correctement configuré, vous entendez une sonnerie de téléphone et, après un bref instant, vous entendez une courte annonce.

SI vous avez terminé cette procédure avec succès, vous pouvez être sûr que votre configuration audio et que votre réseau fonctionnent. Si ce test échoue, vérifiez si votre périphérique audio est correctement configuré et si le niveau de lecture est réglé sur une valeur raisonnable. Si vous n'entendez toujours rien, vérifiez la configuration du réseau, y compris les numéros de port SIP et RTP. Si une autre application ou un autre protocole utilise les ports par défaut proposés par Linphone, changez les ports et réessayez.

5.3 Appel d'un correspondant

Il est très simple d'appeler un correspondant lorsque Linphone est correctement configuré. Selon le type d'appel (consultez la Section 5.1.2, « Détermination du type de connexion » (p. 96)), les procédures diffèrent légèrement.

1. Démarrez Linphone depuis le menu ou par une ligne de commande.
2. Saisissez l'adresse SIP du correspondant à l'invite *SIP address (Adresse SIP)*. L'adresse doit ressembler à `sip:nomd'utilisateur@nomdedomaine` ou `nomd'utilisateur@nomd'hôte` pour les appels locaux directs ou à

`nomd'utilisateur@serveursip` ou `idutilisateur@serveursip` pour les appels proxy ou ceux utilisant le service d'un fournisseur SIP.

3. Si vous utilisez un fournisseur de services SIP ou un proxy, sélectionnez le proxy ou le fournisseur approprié dans *Proxy to use (Proxy à utiliser)* et fournissez les informations d'authentification requises par ce proxy.

4. Cliquez sur *Call or Answer (Appeler ou répondre)* et attendez que votre correspondant décroche.

5. Lorsque vous avez terminé ou que souhaitez mettre fin à la communication, cliquez sur *Release or Refuse (Libérer ou refuser)* et quittez Linphone.

Si vous devez régler les paramètres audio au cours d'une communication, cliquez sur *Show more (Plus)* pour afficher quatre onglets contenant davantage d'options. Le premier contient les options *Son* de *Playback level (Niveau de lecture)* et de *Recording level (Niveau d'enregistrement)*. Utilisez les curseurs pour régler les deux volumes selon vos besoins.

L'onglet *Presence (Présence)* permet de définir votre statut en ligne. Ces informations peuvent être relayées vers quiconque tente de vous contacter. Si vous vous absentez définitivement et souhaitez en informer votre correspondant, il suffit de cocher *Away (Absent)*. Si vous êtes simplement occupé, et souhaitez que votre correspondant essaie de nouveau de vous appeler, cochez *Busy, I'll be back in ... min (Occupé, de retour dans ... minutes)* et précisez la durée pendant laquelle vous ne pourrez être joint. Lorsqu'on peut vous joindre à nouveau, rétablissez le paramètre par défaut *Reachable (Joignable)*. La possibilité pour un autre correspondant de connaître votre statut en ligne est déterminée par la *Subscribe Policy (Politique d'inscription)* définie dans le carnet d'adresses, comme indiqué dans Section 5.5, « Utilisation du carnet d'adresses » (p. 103). Si un correspondant de votre carnet d'adresses a publié son statut en ligne, vous pouvez le surveiller dans l'onglet *My online friends (Mes amis en ligne)*.

L'onglet *DTMF* permet de saisir les codes DTMF pour consulter la messagerie vocale. Pour consulter votre messagerie vocale, saisissez l'adresse SIP appropriée et utilisez le clavier de l'onglet *DTMF* pour saisir le code de la messagerie vocale. Enfin, cliquez sur *Call or Answer (Appeler ou répondre)* comme si vous appeliez un correspondant ordinaire.

5.4 Réponse à un correspondant

Selon le mode d'exécution sélectionné pour Linphone, il existe plusieurs manières de remarquer un appel entrant :

Application normale
Vous ne pouvez recevoir des appels et y répondre que si Linphone est en cours d'exécution. Vous entendez alors la sonnerie du téléphone dans vos écouteurs ou vos haut-parleurs. Lorsque Linphone n'est pas en cours d'exécution, l'appel ne peut être reçu.

Panneau de configuration GNOME
Normalement, l'applet du tableau de bord Linphone doit s'exécuter automatiquement sans signaler sa présence. Ceci change dès qu'un appel entre : la fenêtre principale de Linphone s'ouvre et vous entendez une sonnerie de téléphone dans vos écouteurs ou vos haut-parleurs.

Lorsque vous avez remarqué un appel entrant, il vous suffit de cliquer sur *Call or Answer (Appeler ou répondre)* pour prendre l'appel et commencer à parler. Si vous ne souhaitez pas prendre cet appel, cliquez sur *Release or Refuse (Libérer ou refuser)*.

5.5 Utilisation du carnet d'adresses

Linphone vous propose de gérer vos contacts SIP. Cliquez sur *Aller → Address book (Carnet d'adresses)* pour démarrer le carnet d'adresses. Une fenêtre de liste vide s'ouvre. Cliquez sur *Ajouter* pour ajouter un contact.

Les entrées suivantes sont nécessaires pour qu'un contact soit valide :

Nom
Saisissez le nom du contact. Il peut s'agit d'un nom entier ou d'un surnom. Choisissez un nom facile à retenir. Si vous choisissez de voir le statut en ligne de cette personne, ce nom apparaît dans l'onglet *My online friends (Mes amis en ligne)* de la fenêtre principale.

Adresse SIP
Saisissez une adresse SIP valide pour votre contact.

Proxy à utiliser
Si nécessaire, saisissez le proxy à utiliser pour cette connexion particulière. Dans la plupart des cas, il doit s'agir uniquement de l'adresse SIP du serveur SIP que vous utilisez.

Politique d'abonnement
Votre politique d'abonnement détermine si votre présence ou votre absence peuvent être surveillées par d'autres utilisateurs.

Pour appeler un contact du carnet d'adresses, sélectionnez-le avec la souris, cliquez sur *Sélectionner* pour que l'adresse apparaisse dans le champ d'adresse de la fenêtre principale, et démarrez normalement l'appel avec *Call or Answer (Appeler ou répondre)*.

5.6 Dépannage

Je tente d'appeler un correspondant, mais la connexion ne s'établit pas.
Il existe plusieurs raisons pour lesquelles un appel peut échouer :

Votre connexion sur Internet est rompue.
Du fait que Linphone utilise Internet pour relayer vos appels, vérifiez que votre ordinateur est correctement connecté et configuré sur Internet. Ceci peut être testé facilement en tentant d'afficher une page Web dans votre navigateur. Si la connexion Internet fonctionne, il se peut que votre correspondant ne soit pas joignable.

La personne que vous tentez d'appeler n'est pas joignable.
Si votre correspondant a refusé votre appel, vous ne pouvez être connecté. Si Linphone n'est pas en cours d'exécution sur la machine de votre correspondant au moment où vous l'appelez, vous ne pouvez être connecté. Si la connexion Internet de votre correspondant est rompue, vous ne pouvez être connecté.

Mon appel semble se connecter, mais je n'entends rien.
Vérifiez d'abord que votre périphérique audio est correctement configuré. Lancez pour cela une autre application utilisant une sortie audio, par exemple un lecteur multimédia. Vérifiez que Linphone dispose des autorisations suffisantes pour ouvrir ce périphérique. Fermez tous les programmes utilisant le périphérique audio pour éviter des conflits de ressources.

Si toutes les vérifications ci-dessus n'ont révélé aucune anomalie et si vous n'entendez toujours rien, augmentez les volumes d'enregistrement et de lecture dans l'onglet *Son*.

La sortie vocale aux deux extrémités semble étrangement tronquée.
Tentez de régler le tampon d'instabilité en utilisant *RTP properties (Propriétés RTP)* dans *Préférences* → *Réseau* pour compenser les paquets vocaux retardés. Lorsque vous faites cela, n'oubliez pas que vous augmentez la latence.

DTMF ne fonctionne pas.
Vous avez tenté de consulter votre messagerie vocale à l'aide du clavier DTMF, mais la connexion n'a pu être établie. Trois protocoles différents existent pour la transmission des données DTMF, mais seulement deux d'entre eux sont pris en charge par Linphone (SIP INFO et RTP rfc2833). Vérifiez auprès de votre fournisseur s'il prend en charge l'un de ces deux protocoles. Le protocole par défaut utilisé par Linphone est rfc2833, mais en cas d'échec, vous pouvez définir le protocole sur SIP INFO dans *Préférences* → *Réseau* → *Autre*. Si aucun d'entre eux ne fonctionne, la transmission DTMF n'est pas possible avec Linphone.

5.7 Glossaire

Vous trouverez ci-dessous une brève explication des termes techniques et protocoles les plus importants mentionnés dans ce document :

codec
Les codecs sont des algorithmes spécialement conçus pour compresser les données audio et vidéo.

DTMF
Un codeur DTMF, comme un téléphone ordinaire, utilise des paires de tonalités pour représenter les différentes touches. Chaque touche est associée à une combinaison unique d'une tonalité aiguë et d'une tonalité grave. Un décodeur retraduit ensuite ces combinaisons en nombre. Linphone prend en charge la signalisation DTMF pour déclencher des actions distantes, telles que la consultation de la messagerie vocale.

instabilité
L'instabilité est l'écart de latence (retard) dans une connexion. Les périphériques audio ou les systèmes à connexion, tels que ISDN ou PSTN, nécessitent un flux de

données continu. Pour compenser cela, les terminaux et passerelles VoIP implémentent un tampon d'instabilité qui collecte les paquets avant de les relayer sur leurs périphériques audio ou leurs lignes orientées connexion (telles que ISDN). Le fait d'augmenter la taille du tampon d'instabilité réduit la probabilité de perte de données, mais la latence de la connexion augmente.

RTP

RTP signifie *real-time transport protocol (protocole de transport en temps réel)*. Il permet le transport des flux multimédia sur les réseaux et fonctionne sur UDP. Les données sont transmises au moyen de paquets discrets qui sont numérotés et transportent un tampon horaire afin de permettre le séquencement et la détection corrects des paquets perdus.

SIP

VoIP signifie *session initiation protocol (protocole d'ouverture de session)*. Ce protocole est utilisé pour établir des sessions multimédia sur les réseaux. Dans le contexte Linphone, SIP est la magie qui déclenche la sonnerie sur la machine de votre correspondant, démarre l'appel et le termine dès que l'un des interlocuteurs décide de raccrocher. La transmission réelle des données vocales est gérée par RTP.

VoIP

VoIP signifie *voice over Internet protocol (voix sur protocole Internet)*. Cette technologie permet la transmission des appels téléphoniques ordinaires sur Internet en utilisant des routes liées aux paquets. Les informations vocales sont envoyées dans des paquets discrets comme n'importe quelle autre données transmise sur Internet via IP.

5.8 Pour plus d'informations

Pour obtenir des informations générales concernant VoIP, consultez VoIP Wiki à l'adresse `http://voip-info.org/tiki-index.php`. Pour consulter la liste complète des fournisseurs offrant des services VoIP dans votre pays, consultez `http://voip-info.org/wiki-VOIP+Service+Providers+Residential`.

6 Le chiffrement avec KGpg

KGpg est un important composant de l'infrastructure de chiffrement de votre système. Ce programme permet de générer et de gérer toutes les clés nécessaires. Utilisez ses fonctions d'éditeur pour rapidement créer et chiffrer vos fichiers, ou utilisez l'applet dans votre panneau pour chiffrer et déchiffrer en utilisant le glisser-déposer. D'autres programmes, tels que votre programme de messagerie (Kontact ou Evolution), accèdent aux données de clé afin de traiter des contenus signés ou chiffrés. Ce chapitre présente les fonctions élémentaires nécessaires à la gestion quotidienne de fichiers chiffrés.

6.1 Génération d'une nouvelle paire de clés

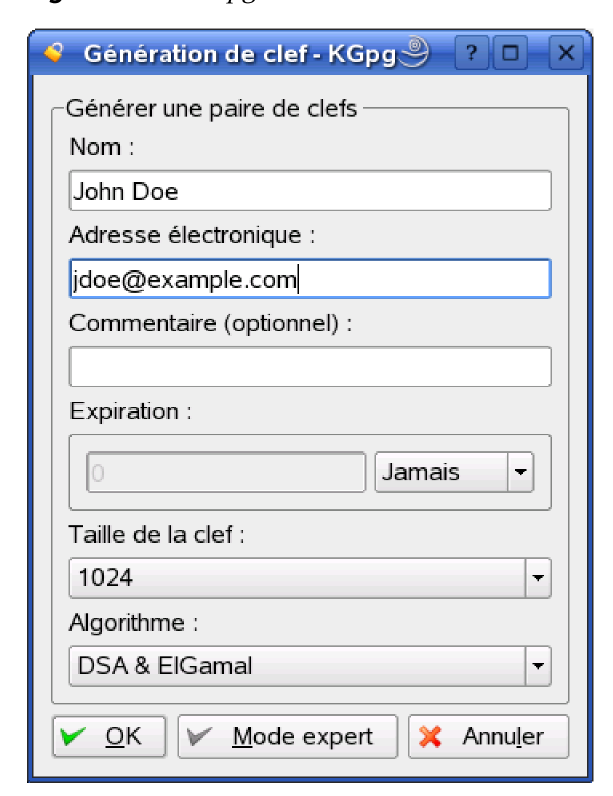
Pour pouvoir échanger des messages chiffrés avec d'autres utilisateurs, vous devez d'abord générer votre propre paire de clés. Le premier composant de la paire, à savoir la *clé publique*, est distribué à vos partenaires de communication, qui peuvent l'utiliser pour chiffrer les fichiers ou les messages électroniques qu'ils envoient. L'autre composant, *la clé privée*, sert à déchiffrer le contenu chiffré.

IMPORTANT: Clé privée VS clé publique

La clé publique est destinée au public, c'est-à-dire qu'elle doit être distribuée à l'ensemble de vos partenaires de communication. La clé privée, au contraire, ne peut être connue que de vous. Les autres utilisateurs ne peuvent pas avoir accès à cette information.

Lancez KGpg à partir du menu principal en sélectionnant *Utilitaires* → *KGpg* ou en entrant `kgpg` dans la ligne de commande. La première fois que vous démarrez ce programme, un Assistant apparaît pour vous guider lors de la procédure de configuration. Suivez les instructions jusqu'à l'étape où vous êtes invité à créer une clé. Entrez un nom, une adresse électronique et, éventuellement, un commentaire. Si les paramètres par défaut fournis ne vous conviennent pas, définissez également la date d'expiration de la clé, sa taille et l'algorithme de chiffrement utilisé. (voir Figure 6.1, « KGpg : création d'une clé » (p. 108)).

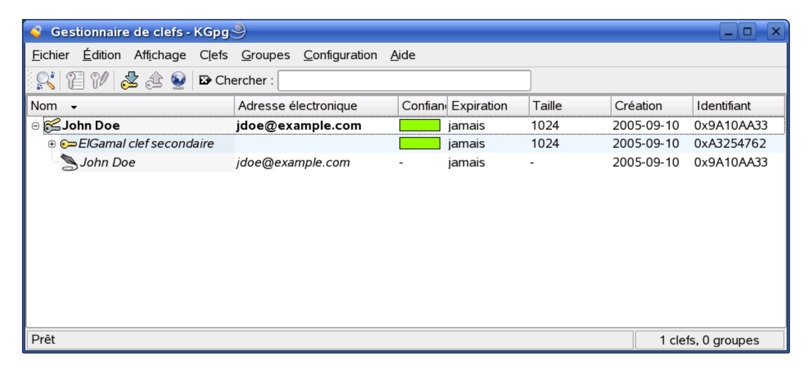
Figure 6.1 *KGpg : création d'une clé*



Cliquez sur *OK* pour confirmer vos paramètres. Dans la boîte de dialogue suivante, le système vous invite à saisir deux fois votre mot de passe. Le programme génère ensuite la paire de clés et affiche un résumé. N'oubliez pas d'enregistrer ou d'imprimer immédiatement le certificat de révocation. Vous aurez besoin de ce certificat si vous oubliez le mot de passe de votre clé privée et si vous devez révoquer cette dernière.

Cliquez sur *OK* pour confirmer vos paramètres. KGpg affiche alors sa fenêtre principale. (voir Figure 6.2, « Le gestionnaire de clés » (p. 109)).

Figure 6.2 *Le gestionnaire de clés*



6.2 Exportation de la clé publique

Après avoir généré votre paire de clés, vous devez mettre la clé publique à disposition des autres utilisateurs. Ils pourront ainsi utiliser la clé pour chiffrer ou signer les messages et les fichiers qu'ils vous envoient. Pour mettre la clé publique à disposition d'autrui, sélectionnez *Keys (Clés)* → *Export Public Key(s) (Exporter la clé publique)*. La boîte de dialogue qui s'ouvre vous propose quatre options :

Email (Courrier électronique)

Votre clé publique est envoyée par courrier électronique au destinataire de votre choix. Si vous activez cette option et confirmez votre choix en cliquant sur *OK*, la boîte de dialogue de création d'un message électronique KMail apparaît. Tapez le nom du destinataire et cliquez sur *Envoyer*. Le destinataire reçoit votre clé et peut ensuite vous envoyer du contenu chiffré.

Clipboard (Presse-papiers)

Vous pouvez placer votre clé publique dans le Presse-papiers avant de l'utiliser.

Default Key Server (Serveur de clés par défaut)

Pour mettre votre clé publique à disposition du grand public, exportez-la sur un des serveurs de clés sur Internet. Pour plus d'informations, reportez-vous à Section 6.4, « La boîte de dialogue Serveur de clés » (p. 111).

Fichier

Si vous préférez distribuer votre clé sous la forme d'un fichier stocké sur un support de données au lieu de l'envoyer par courrier électronique, activez cette option, confirmez les valeurs par défaut ou modifiez le chemin d'accès et le nom du fichier et cliquez sur *OK*.

6.3 Importation de clés

Si vous recevez une clé dans un fichier (par exemple, dans une pièce jointe à un message électronique), intégrez-la à votre trousseau grâce à *Import Key (Importer la clé)* et utilisez-la pour chiffrer vos communications avec son expéditeur. Cette procédure ressemble à la procédure d'exportation de clés décrite précédemment.

6.3.1 Signature de clés

Les clés peuvent être signées comme tout autre fichier afin de garantir leur authenticité et intégrité. Si vous êtes absolument certain qu'une clé importée appartient à l'individu indiqué comme son propriétaire, marquez votre confiance dans l'authenticité de la clé avec votre signature.

IMPORTANT: Établissement d'un Web de confiance

Une communication chiffrée n'est sécurisée que lorsque vous êtes certain de pouvoir associer des clés publiques en circulation avec l'utilisateur spécifié. En vérifiant et en signant ces clés, vous contribuez à la promotion d'un Web de confiance.

Sélectionnez la clé à signer dans la liste de clés. Sélectionnez *Keys (Clé) → Sign Keys (Signer la clé)*. Dans la boîte de dialogue suivante, spécifiez la clé privée à utiliser pour la signature. Une alerte vous rappelle de vérifier l'authenticité de cette clé avant de la signer. Si vous avez bien effectué cette vérification, cliquez sur *Continue (Continuer)* et à l'étape suivante, tapez le mot de passe correspondant à la clé privée sélectionnée. D'autres utilisateurs pourront désormais vérifier votre signature au moyen de votre clé publique.

6.3.2 Approbation d'une clé

Normalement, le programme correspondant vous demande si vous approuvez la clé (si vous estimez qu'elle est réellement utilisée par son propriétaire autorisé). Cela se produit chaque fois qu'un message a besoin d'être déchiffré ou qu'une signature doit être contrôlée. Pour éviter cette procédure, modifiez le niveau d'approbation de la clé nouvellement importée.

Cliquez avec le bouton droit de la souris sur la nouvelle clé pour accéder à un petit menu contextuel de gestion des clés. Sélectionnez *Edit Key in Terminal (Modifier la clé en terminal)*. KGpg ouvre une console de texte dans laquelle vous pouvez définir le niveau de confiance à l'aide de quelques commandes.

À l'invite de la console (`Command >`), tapez `trust`. Sur une échelle allant de `1` (non fiable) à `5` (confiance absolue), estimez le degré de confiance que vous avez dans le fait que les signataires de la clé importée ont contrôlé la véritable identité du propriétaire de cette clé. Tapez la valeur sélectionnée à l'invite (`Your décision?` (Votre décision ?)). Si vous êtes véritablement sûr de la confiance des signataires, entrez `5`. Répondez à la question suivante en tapant `y`. Pour terminer, tapez `quit` pour quitter la console et revenir à la liste de clés. La clé a désormais le niveau d'approbation `Ultimate` (Ultime).

Le niveau de confiance des clés de votre trousseau est indiqué par une barre de couleur en regard du nom de cette clé. Plus le niveau de confiance est faible, moins vous faites confiance au signataire d'avoir contrôlé la véritable identité des clés signées. Vous pouvez être tout à fait certain de l'identité du signataire, mais il se peut qu'il soit paresseux et qu'il n'ait pas contrôlé l'identité des autres personnes avant la signature de leurs clés. Par conséquent, vous pouvez très bien lui faire confiance à lui et à sa propre clé, mais assigner des niveaux de confiance inférieurs aux clés des autres qu'il a signées. Les niveaux de confiance sont proposés uniquement à titre de rappel. Ils ne déclenchent aucune opération automatique dans KGpg.

6.4 La boîte de dialogue Serveur de clés

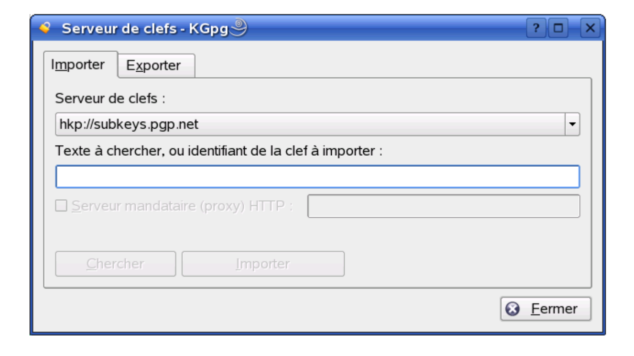
Plusieurs serveurs de clés basés sur Internet offrent les clés publiques de nombreux utilisateurs. Pour entamer une communication chiffrée avec un grand nombre

d'utilisateurs, utilisez ces serveurs afin de leur distribuer votre clé publique. Pour ce faire, exportez votre clé publique sur un de ces serveurs. De manière similaire, KGpg permet d'effectuer une recherche sur un de ces serveurs afin de retrouver et d'importer les clés publiques du serveur. Ouvrez la boîte de dialogue du serveur de clés à l'aide de *File (Fichier)* → *Key Server Dialog (Serveur de clés)*.

6.4.1 Importation d'une clé à partir d'un serveur de clés

L'onglet *Importer* de la boîte de dialogue Serveur de clés permet d'importer des clés publiques à partir d'un des serveurs de clés basés sur Internet. Utilisez son menu déroulant pour sélectionner un des serveurs de clés préconfigurés et tapez une chaîne de recherche (l'adresse électronique du partenaire de communication) ou l'identifiant de la clé afin de la retrouver. Lorsque vous cliquez sur *Recherche*r, votre système se connecte à Internet et recherche une clé correspondant à vos critères sur le serveur de clés spécifié. Voir Figure 6.3, « Écran de recherche pour l'importation d'une clé » (p. 112).

Figure 6.3 *Écran de recherche pour l'importation d'une clé*



Si votre recherche sur le serveur de clés a réussi, une liste de toutes les entrées correspondantes récupérées apparaît dans une nouvelle fenêtre. Sélectionnez la clé que vous voulez ajouter à votre trousseau et cliquez sur *Importer*. (voir Figure 6.4, « Occurrences et Importation » (p. 113)). Confirmez le message suivant en cliquant sur *OK*, puis quittez la boîte de dialogue Serveur de clés en cliquant sur *Fermer*. La clé importée apparaît ensuite dans la vue d'ensemble générale du gestionnaire de clés, prête à l'emploi.

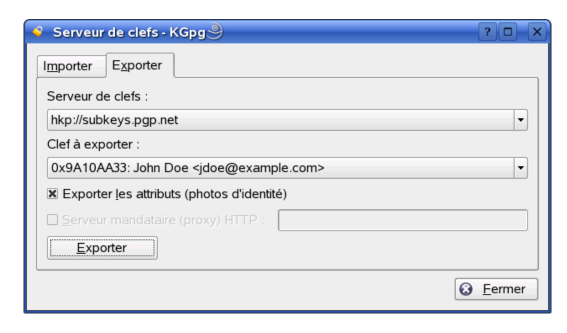
Figure 6.4 *Occurrences et Importation*



6.4.2 Exportation de vos clés vers un serveur de clés

Pour exporter votre clé sur l'un des serveurs de clés gratuits d'Internet, sélectionnez l'onglet *Export (Exporter)* dans la boîte de dialogue du serveur de clés. Désignez le serveur cible et la clé à exporter au moyen des deux menus déroulants. Lancez ensuite l'exportation en cliquant sur *Exporter*.

Figure 6.5 *Exportation d'une clé vers un serveur de clés*



6.5 Chiffrement de texte et de fichiers

KGpg offre également la possibilité de chiffrer du texte ou le contenu du presse-papiers. Cliquez sur le cadenas pour afficher les options *Encrypt clipboard (Chiffrer le Presse-papiers)* et *Decrypt clipboard (Déchiffrer le Presse-papiers)*, ainsi que l'option permettant d'ouvrir l'éditeur intégré.

6.5.1 Chiffrement et déchiffrement du presse-papiers

Les fichiers copiés dans le presse-papiers peuvent être facilement chiffrés en quelques clics. Ouvrez la vue d'ensemble des fonctions en cliquant sur l'icône KGpg. Sélectionnez *Chiffrer le Presse-papiers* et choisissez la clé à utiliser. Un message d'état concernant la procédure de chiffrement s'affiche sur le bureau. Vous pouvez désormais traiter le contenu chiffré à partir du presse-papiers selon vos besoins. Le déchiffrement du contenu du presse-papiers est aussi simple. Il suffit d'ouvrir le menu dans le panneau, de sélectionner *Decrypt Clipboard (Déchiffrer le Pressepapiers)* et de taper le mot de passe associé à votre clé privée. Vous pouvez ensuite utiliser la version déchiffrée à partir du presse-papiers ou de l'éditeur KGpg.

6.5.2 Chiffrement et déchiffrement par glisser-déposer

Pour chiffrer ou déchiffrer des fichiers, cliquez sur leur icône sur le bureau ou sur leur nom dans le gestionnaire de fichiers, glissez-les sur le cadenas dans le panneau et déposez-les. Si le fichier n'est pas chiffré, KGpg vous demande de choisir une clé. Une fois que vous avez sélectionné une clé, le fichier est chiffré sans autre message. Dans le gestionnaire de fichiers, les fichiers chiffrés sont reconnaissables au suffixe `.asc` et au petit cadenas. Pour déchiffrer ces fichiers, cliquez sur leur icône, glissez-les sur le symbole KGpg dans le panneau et déposez-les. Ensuite, choisissez entre chiffrer, enregistrer ou afficher le fichier dans l'éditeur.

6.5.3 L'éditeur KGpg

Au lieu de créer un fichier et de le chiffrer dans un éditeur externe selon l'une des méthodes décrites ci-dessus, vous pouvez utiliser l'éditeur intégré de KGpg pour créer le fichier. Ouvrez l'éditeur (*Ouvrir l'éditeur* dans le menu contextuel), tapez le texte voulu et cliquez sur *Chiffrer*. Ensuite, sélectionnez la clé à utiliser et effectuez le reste de la procédure de chiffrement. Pour déchiffrer les fichiers, cliquez sur *Déchiffrer* et tapez le mot de passe associé à la clé.

La génération et la vérification de signatures sont aussi simples que le chiffrement direct à partir de l'éditeur. Allez dans *Signature → Générer une signature* et sélectionnez le fichier à signer dans la boîte de dialogue de fichiers. Ensuite, spécifiez la clé privée à utiliser et tapez le mot de passe correspondant. KGpg vous informe que la génération de la signature a réussi. Vous pouvez également signer vos fichiers à partir de l'éditeur en cliquant simplement sur *Signer / Vérifier*. Pour vérifier un fichier signé, allez dans *Signature → Vérifier une signature* et sélectionnez le fichier à vérifier dans la boîte de dialogue suivante. Dès que vous confirmez cette sélection, KGpg vérifie la signature et vous informe du résultat de l'opération. Une autre possibilité consiste à charger le fichier signé dans l'éditeur et à cliquer sur *Signer / Vérifier*.

6.6 Pour plus d'informations

Pour obtenir des informations théoriques de fond sur la méthode de chiffrement, reportez-vous à la présentation claire et succincte des pages du projet GnuPG sur http://www.gnupg.org/documentation/howtos.html.en. Ce site offre également une liste de sources d'informations complémentaires.



Multimédia

7

Son dans Linux

Linux intègre une large gamme d'applications sonores et multimédias. Certaines de ces applications font partie d'un des environnements de bureau les plus courants. Avec les applications décrites ici, vous contrôlez le volume, la balance ou la lecture, vous lisez des CD et des fichiers musicaux, et vous pouvez enregistrer et compresser vos propres données audio.

7.1 Mixeurs

Un mixeur est un outil pratique qui permet de contrôler facilement le volume et la balance de la sortie et de l'entrée audio d'un ordinateur. Les différentes consoles de mixage se distinguent par l'apparence extérieure de leur interface utilisateur. Cependant, certains mixeurs sont conçus pour du matériel spécifique. C'est notamment le cas d'envy24control, un mixeur conçu pour la puce son Envy 24. Destiné aux cartes RME Hammerfall, hdspmixer est un autre exemple. Sélectionnez, parmi les mixeurs disponibles, celui qui correspond le mieux à vos besoins.

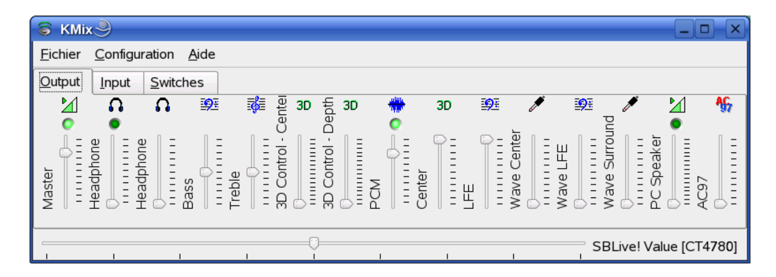
ASTUCE: Test du mixeur

Généralement, il est préférable d'ouvrir l'application de mixage avant toute autre application sonore. Utilisez le mixeur pour tester et régler les paramètres de contrôle d'entrée et de sortie de la carte son.

7.1.1 L'applet de mixage de KDE

KMix est l'application de mixage de KDE. Elle est intégrée au tableau de bord KDE, sous la forme d'une petite applet située dans la barre système. Cliquez sur l'icône de tableau de bord pour régler le volume des haut-parleurs à l'aide d'une glissière. Si vous cliquez avec le bouton droit de la souris sur l'icône, le menu contextuel de KMix apparaît. Sélectionnez *Mute* (Muet) pour couper le son. L'icône de tableau de bord change d'apparence. Pour remettre le son, cliquez de nouveau sur *Mute*. Pour régler plus précisément les paramètres sonores, sélectionnez *Show Mixer Window* (Afficher la fenêtre de mixeur) et configurez les options *Output* (Sortie), *Input* (Entrée) et *Switches* (Interrupteurs). Chacun des périphériques indiqués ici possède son propre menu contextuel, accessible en cliquant avec le bouton droit de la souris sur l'icône du périphérique concerné. Vous pouvez les masquer ou les rendre muets un par un.

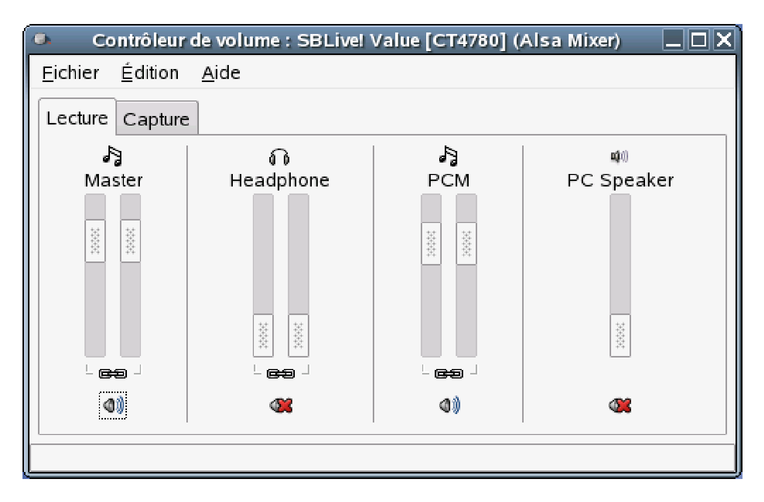
***Figure 7.1** Le mixeur KMix*



7.1.2 L'applet de mixage de GNOME

GMix, l'applet de contrôle de volume du bureau GNOME, est intégrée dans le tableau de bord GNOME. Cliquez sur l'icône de tableau de bord pour régler le volume des haut-parleurs à l'aide d'une glissière. Pour couper le son, cliquez sur l'icône avec le bouton droit de la souris et sélectionnez *Mute* (Muet). L'icône de contrôle de volume change d'apparence. Pour remettre le son, cliquez de nouveau sur l'icône avec le bouton droit de la souris et sélectionnez *Mute* (Muet) dans le menu. Sélectionnez *Open Volume Control* (Ouvrir le contrôle de volume) pour accéder aux fonctionnalités avancées du mixeur, affichées à la Figure 7.2, « L'applet de mixage de GNOME » (p. 121). Chaque périphérique sonore a son propre onglet de mixage.

Figure 7.2 *L'applet de mixage de GNOME*



7.1.3 alsamixer

Vous pouvez exécuter alsamixer sur la ligne de commande, hors de l'environnement X, afin de le contrôler entièrement par des raccourcis clavier. La fenêtre alsamixer se compose toujours des éléments suivants : une ligne supérieure contenant des informations de base sur le type de carte et de puce, le type d'affichage sélectionné, puis le mixeur et les barres de volume, sous la zone d'informations. Utilisez ← et → pour vous déplacer vers la gauche ou la droite, si les contrôles ne peuvent pas être affichés dans un seul écran. Les noms des contrôles apparaissent sous ces derniers et le contrôle sélectionné est coloré en rouge. Coupez ou rétablissez le son de n'importe quel contrôle de mixage, à l'aide de M. Lorsqu'un contrôle est muet, la mention *MM* figure sous son nom. Tout contrôle qui possède des fonctionnalités de capture (enregistrement) porte un indicateur de capture rouge.

alsamixer propose trois modes d'affichage : *Playback* (Lecture), *Capture* (Enregistrement) et *All* (Tout). Par défaut, alsamixer démarre en mode *Playback* (Lecture) et n'affiche que les contrôles de mixage qui concernent la lecture (volume principal, PCM, CD, etc.). Le mode *Capture* (Enregistrement) affiche uniquement les contrôles d'enregistrement. Le mode *All* (Tout) affiche tous les contrôles disponibles. Vous passez d'un mode d'affichage à l'autre avec les touches F3, F4 et F5.

Sélectionnez des canaux avec → et ←, ou N et P. Les touches ↑ et ↓, ou + et -, augmentent ou réduisent le volume. Les canaux stéréo peuvent être contrôlés indépendamment, avec Q, W et E (pour augmenter le volume), et avec Z, X et C (pour le réduire). Les touches numérotées (0 à 9) peuvent servir à modifier rapidement le volume absolu. Elles indiquent un volume qui va de 0 à 90 % du volume maximum.

7.1.4 Apparence des applications de mixage

L'apparence et le style des applications de mixage dépendent du type de carte son utilisé. Certains pilotes, comme SB Live!, comportent de nombreux éléments de mixeur réglables, alors que les pilotes de cartes son professionnelles peuvent présenter des éléments portant des noms complètement différents.

Puce son intégrée

La plupart des puces son PCI intégrées sont basées sur le codec AC97. L'option *Master* (Maître) contrôle le volume principal des haut-parleurs avant. Les options *Surround* (Contour), *Center* (Centre) et *LFE* (Ampli basses fréquences) contrôlent les haut-parleurs arrière, centraux et basses fréquences. Chacun possède un interrupteur Mute (Muet). De plus, certaines cartes ont des contrôles de volume *Headphone* (Casque) et *Master Mono* (Mono maître) distincts. Ce dernier sert au haut-parleur intégré dans certains portables.

L'option *PCM* contrôle le niveau de volume interne de la lecture WAVE numérique. L'acronyme PCM signifie Pulse Code Modulation (Modulation par impulsions et codage), l'un des formats de signal numérique. Ce contrôle comporte également un interrupteur Mute (Muet) séparé.

D'autres contrôles, comme *CD*, *Line* (Ligne), *Mic* et *Aux*, contrôlent le volume de boucle de l'entrée correspondante vers la sortie principale. Ils n'influencent pas le niveau d'enregistrement, uniquement les volumes de lecture.

Pour enregistrer, activez l'interrupteur *Capture* (Enregistrement). Il s'agit de l'interrupteur d'enregistrement principal. Le volume de *Capture* est le gain d'entrée de l'enregistrement. Par défaut, cet interrupteur est réglé sur zéro. Choisissez une source d'enregistrement, comme *Line* (Ligne) ou *Mic* (Micro). La source d'enregistrement est exclusive, vous ne pouvez donc pas en choisir deux à la fois. La source *Mix* est une source d'enregistrement spéciale. Cette source permet d'enregistrer le signal en cours de lecture.

En fonction de la puce codec AC97, des effets spéciaux, comme le 3D ou le réglage Basses/Aigus sont également disponibles.

SoundBlaster Live! et la gamme Audigy

SoundBlaster Live! et SB Audigy1 possèdent de nombreux contrôles de mixage pour leur puce codec AC97 et leur moteur DSP. Outre les contrôles décrits précédemment, ils offrent des options *Wave*, *Music* et *AC97* pour contrôler l'atténuation et le routage du signal interne pour le mixage PCM, WaveTable MIDI et AC97. Laissez le volume à 100 % pour tous les entendre. SB Audigy2 (selon le modèle) possède moins de contrôles que SB Live, mais offre au moins les options *Wave* et *Music*.

L'enregistrement avec SB Live fonctionne pratiquement comme avec une puce intégrée. Vous pouvez choisir *Wave* et *Music* comme source d'enregistrement supplémentaire pour enregistrer les signaux PCM et WaveTable.

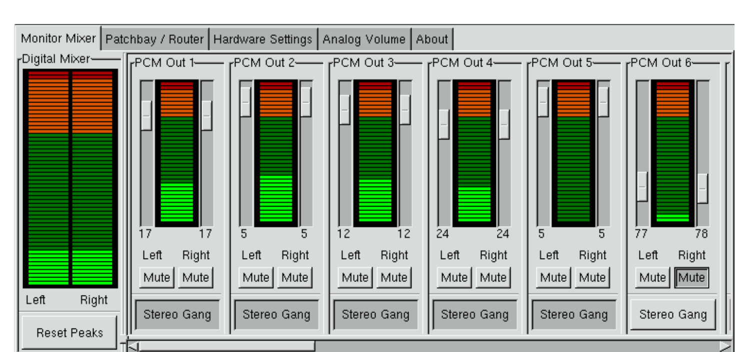
Périphériques audio USB

Les périphériques audio USB ont généralement peu de contrôles de mixage. Parfois même, ils n'en n'ont aucun. La plupart des périphériques ont un interrupteur *Master* (Maître) ou *PCM* pour contrôler le volume de lecture.

7.1.5 Le mixeur pour la puce son Envy24

envy24control est une application de mixage pour les cartes son qui utilisent la puce Envy24 (ice1712). La flexibilité de la puce Envy24 entraîne une certaine variation au niveau des fonctionnalités offertes par les différentes cartes son. Les dernières informations concernant cette puce sont rassemblées sous `/usr/share/doc/packages/alsa/alsa-tools/envy24control`.

Figure 7.3 *Moniteur et mixeur numérique de envy24control*



Le *Monitor Mixer* de envy24control montre les niveaux de signaux qui peuvent être mixés numériquement dans la carte son. Les signaux dits *PCM Out* sont générés par des applications qui envoient des données PCM à la carte son. Les signaux émis par les entrées analogiques sont regroupés sous *H/W In*. Les entrées *S/PDIF* se situent à droite. Définissez les niveaux d'entrée et de sortie des canaux analogiques sous *Analog Volume* (Volume analogique).

Utilisez les glissières du *Monitor Mixer* pour le mixage numérique. Les niveaux respectifs apparaissent dans le *Digital Mixer* (Mixeur numérique). Pour chaque canal de sortie, le *panneau de raccordement* contient une rangée de cases d'option permettant de sélectionner la source de canal souhaitée.

Réglez l'amplification pour les convertisseurs analogique <-> numérique sous *Analog Volume* (Volume analogique) Les curseurs *DAC* sont destinés aux canaux de sortie, tandis que les curseurs *ADC* sont réservés aux canaux d'entrée.

Les paramètres des canaux S/PDIF sont regroupés sous *Configuration des périphériques*. La puce Envy24 réagit aux changements de volume par un retard qui peut être configuré au moyen de l'option *Volume Change* (Changement de volume).

7.2 Lecteurs multimédias

7.2.1 amaroK

Le lecteur multimédia amaroK peut gérer divers formats audio et lire les flux de diffusion audio des stations de radio sur Internet. Le programme gère tous les types de fichiers pris en charge par le serveur son agissant comme interface dorsale - actuellement aRts ou GStreamer.

Lors du premier démarrage, amaroK lance l'assistant *First-Run Wizard* (Première exécution), qui vous aide à configurer amaroK. Dans un premier temps, configurez l'apparence d'amaroK. Vous pouvez choisir d'afficher le lecteur et la liste de lecture dans deux fenêtres distinctes (consultez la Figure 7.4, « Le lecteur multimédia amaroK » (p. 126)) ou de combiner leurs fonctionnalités dans une fenêtre unique. Dans un deuxième temps, déterminez l'endroit où amaroK doit rechercher votre collection musicale. amaroK recherche dans ces dossiers tous les supports lisibles. Par défaut, amaroK est configuré pour effectuer une recherche récursive au sein des dossiers sélectionnés (afin d'inclure tous les sous-répertoires dans la recherche), pour surveiller les modifications de contenu des répertoires sélectionnés et pour importer toutes les listes de lecture qu'il y trouve. Tous les paramètres configurés avec l'assistant peuvent être modifiés ultérieurement ; pour cela, il suffit de redémarrer l'assistant à l'aide du menu *Tools (outils)* → *First-Run Wizard (Assistant Première exécution)*.

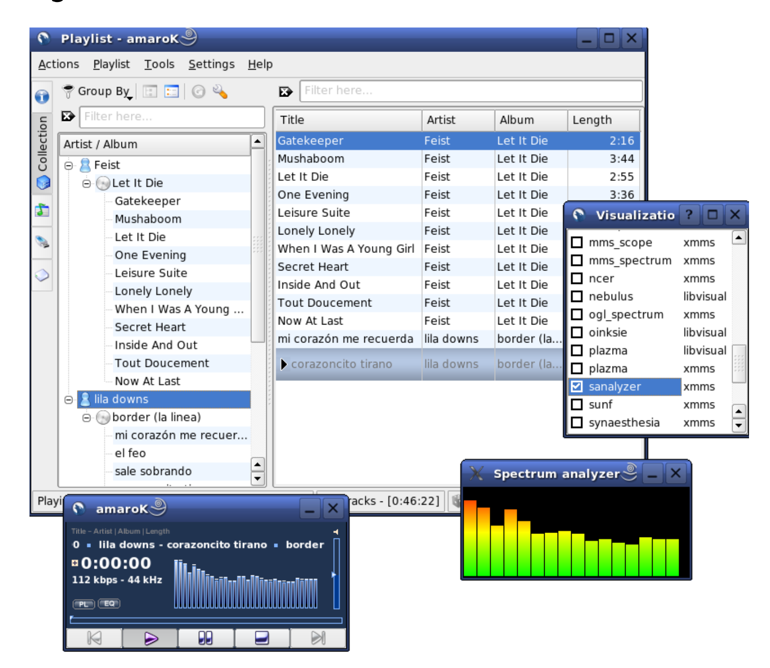


Figure 7.4 *Le lecteur multimédia amaroK*

Administration des listes de lecture

Au démarrage, amaroK balaie le système de fichiers pour trouver des fichiers multimédias, en fonction des paramètres configurés dans l'assistant. La partie droite de la fenêtre répertorie toutes les listes de lecture trouvées. Vous pouvez lire les morceaux qui y figurent dans l'ordre de votre choix. Si aucune liste de lecture n'est trouvée, créez-en une. La meilleure manière d'y parvenir consiste à utiliser la barre latérale à gauche de la fenêtre. À l'extrême gauche, vous trouverez une série d'onglets correspondant à différentes vues. Toutes ces vues vous permettent de sélectionner des morceaux isolés ou des répertoires entiers et de les glisser-déposer dans la liste de lecture. Voici une description de chaque onglet.

Contexte

Cet onglet permet d'afficher des informations sur votre collection et sur la liste actuelle. Par exemple, cette vue vous apprend quels sont vos morceaux préférés, les derniers titres ajoutés à la collection, ainsi que d'autres détails. La vue *Home* (Privé) affiche des statistiques sur vos habitudes d'écoute, répertorie vos morceaux préférés,

les derniers écoutés et ceux que vous écoutez le plus rarement. La zone *Current Track* (Piste actuelle) affiche des données sur le morceau en cours de lecture, comme la couverture de l'album (consultez la section intitulée « Le gestionnaire de couvertures » (p. 128)), les statistiques d'écoute de cette piste et bien d'autres informations. Si vous le souhaitez, vous pouvez afficher les paroles de la chanson à l'aide de l'onglet *Lyrics* (Paroles).

Navigateur de collection

Utilisez cette vue pour gérer et afficher votre collection personnelle de titres. Cette vue peut englober des fichiers situés dans différents emplacements. L'icône représentant une clé dans la barre d'outils permet de déterminer les emplacements de recherche des fichiers musicaux. Une fois les répertoires sélectionnés, la recherche démarre automatiquement. Le résultat apparaît sous forme d'arborescence. Utilisez les options *Primary* (Principal) et *Secondary* (Secondaire) pour organiser les deux branches supérieures de l'arborescence en fonction des critères *Album*, *Artist* (Interprète), *Genre* et *Year* (Année). Une fois l'arborescence terminée, retrouvez des morceaux en tapant simplement leur titre dans le champ d'entrée. Le programme surligne automatiquement, en cours de frappe, la première entrée correspondante. Pour mettre à jour les données de votre collection, lancez une nouvelle recherche dans le système de fichiers avec *Tools (Outils) → Rescan Collection (Rebalayer la collection)*.

Navigateur de listes de lecture

Le navigateur de listes de lecture est divisé en deux parties. La partie supérieure répertorie toutes vos listes personnalisées, créées en faisant glisser des morceaux vers la fenêtre de liste de lecture et en cliquant sur *Save Playlist As* (Enregistrer la liste de lecture sous). Pour afficher leur contenu, cliquez sur + à côté du nom de chaque liste de lecture. Modifiez ces listes de lecture par glisser-déplacer. Pour charger une liste de lecture, double-cliquez dessus.

IMPORTANT: Partage de listes de lecture avec d'autres lecteurs

Vous pouvez enregistrer vos listes de lecture dans le format `m3u` ou `pls` afin de pouvoir les écouter sur n'importe quel autre lecteur prenant en charge ces formats.

---

amaroK peut compiler des listes de lecture utiles (ou « Listes de lecture intelligentes ») à la volée. Utilisez la partie inférieure du navigateur de listes de lecture pour sélectionner l'une des listes intelligentes ou cliquez sur *Create Smart Playlist* (Créer une liste de lecture intelligente) pour définir une liste intelligente person-

nalisée. Saisissez un nom, des critères de recherche, un ordre et (facultatif) une limite de nombre de pistes.

Explorateur de fichiers

Cet onglet ouvre un explorateur de fichiers. Il est identique à la boîte de dialogue de sélection de fichiers standard de KDE et présente les mêmes contrôles de navigation dans le système de fichiers. Tapez une URL ou un répertoire directement dans le champ de saisie de texte. Les pistes qui s'affichent peuvent être ajoutées à la liste de lecture par simple glisser-déplacer. Vous pouvez également effectuer une recherche récursive dans un répertoire spécifique pour trouver un fichier précis. Pour ce faire, tapez une chaîne de texte indiquant le titre et l'emplacement de départ de la recherche. Ensuite, sélectionnez *Rechercher* et patientez quelques secondes. Les résultats apparaissent dans la partie inférieure de la fenêtre.

Le gestionnaire de couvertures

amaroK contient un gestionnaire de couvertures qui vous permet de conserver les données musicales et visuelles qui correspondent à vos albums. Démarrez le *gestionnaire de couverture* via l'option de menu *Tools (Outils) → Cover Manager (Gestionnaire de couverture)*. Une arborescence, à gauche de la fenêtre, répertorie tous les albums de votre collection. Les couvertures récupérées sur Amazon sont affichées dans la partie droite de la fenêtre. A l'aide du menu *View* (Affichage), choisissez le contenu à afficher dans la vue de liste de couvertures. L'option *All albums* (Tous les albums) répertorie tous les albums de votre collection, même s'ils n'ont pas d'image de couverture. L'option *Albums with cover* (Albums avec couverture) répertorie uniquement les albums associés à une couverture et l'option *Albums without cover* (Albums sans couverture) a l'effet inverse. Pour récupérer des données de couverture, accédez au site *Amazon local*, puis cliquez sur l'option permettant de *télécharger les couvertures manquantes*. amaroK essaie d'obtenir les couvertures de tous les albums de votre collection.

Effets

Le bouton *FX* dans la fenêtre du lecteur ou l'option correspondante dans le menu amaroK ouvre une boîte de dialogue qui vous permet d'activer et de configurer plusieurs effets sonores, tels qu'un égaliseur, la balance stéréo ou un effet salle de concert. Sélectionnez les effets souhaités et, le cas échéant, ajustez les paramètres disponibles.

Visualisations

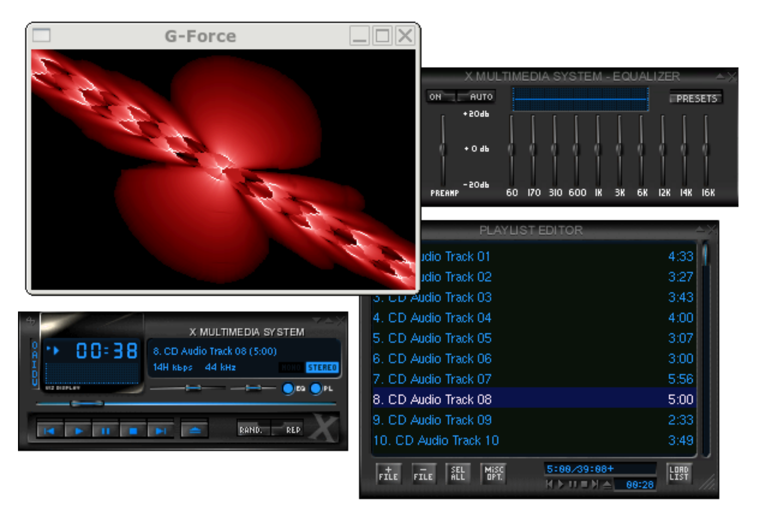
amaroK est fourni avec une série de visualisations qui produisent un effet graphique en fonction de la musique que vous écoutez. Les visualisations amaroK d'origine sont affichées dans la fenêtre du lecteur. Cliquez sur l'animation pour passer d'un mode d'affichage à l'autre.

En outre, amaroK prend en charge les plug-ins de visualisations du lecteur multimédia XMMS. Pour les utiliser, installez d'abord le paquetage `xmms-plugins`, puis sélectionnez *Modules de visualisation* dans le menu de amaroK. La liste des plug-ins disponibles apparaît dans une nouvelle fenêtre. Les plug-ins XMMS sont toujours affichés dans une fenêtre à part. Dans certains cas, vous avez la possibilité de les afficher en mode plein écran. Pour certains plug-ins, l'effet visuel ne sera pas parfait si vous n'utilisez pas une carte graphique 3D accélérée

7.2.2 XMMS

XMMS est un lecteur multimédia ultra complet si performant que les coupures ou autres parasites sont rarissimes pendant la lecture. De plus, l'application est très conviviale. Le bouton permettant d'afficher le menu est situé dans le coin supérieur gauche de la fenêtre du programme. Si vous préférez une apparence de type GNOME, il existe une version GTK2 de XMMS, Beep Media Player. Il suffit d'installer le paquetage `bmp`. Cependant, certains plug-ins XMMS ne sont pas pris en charge par cette version portée de XMMS.

Figure 7.5 *XMMS avec égaliseur, analyseur de spectre OpenGL et plug-ins Infinity*



Sélectionnez le module plug-in de sortie dans *Options* → *Prefences (Préférences)* → *Audio I/O Plugins* (Plug-ins E/S audio). Si vous avez installé le paquetage `xmms-kde`, vous pouvez configurer le serveur de son aRts ici.

IMPORTANT: Utilisation du plug-in d'écriture de disque

XMMS redirige automatiquement sa sortie vers le *plug-in d'écriture de disque* s'il ne trouve pas de carte son configurée. Dans ce cas, les fichiers lus sont écrits sur le disque dur dans le format WAV. Le temps s'écoule donc plus vite que lorsque la sortie est reproduite au travers d'une carte son.

Vous pouvez démarrer plusieurs plug-ins de visualisation avec *Options* → *Preferences (Préférences)* → *Visualization Plugins (Plug-ins de visualisation)*. Si votre ordinateur est équipé d'une carte graphique avec accélération 3D, sélectionnez une application telle que l'analyseur de spectre OpenGL. Si le paquetage `xmms-plugins` est installé, essayez le plugin Infinity.

Les cinq boutons (avec des lettres) situés à gauche en dessous du bouton de menu permettent d'accéder rapidement à d'autres menus, boîtes de dialogue et configurations. Vous ouvrez la liste de lecture avec le bouton *PL* et l'égaliseur avec *EQ*.

7.3 CD : lecture et extraction (RIP)

Il existe de nombreuses manières d'écouter vos morceaux de musique préférés. Vous pouvez lire un CD ou en lire une version numérisée. La section suivante présente quelques applications de lecture de CD, ainsi que des applications d'extraction (RIP) et d'encodage de CD audio.

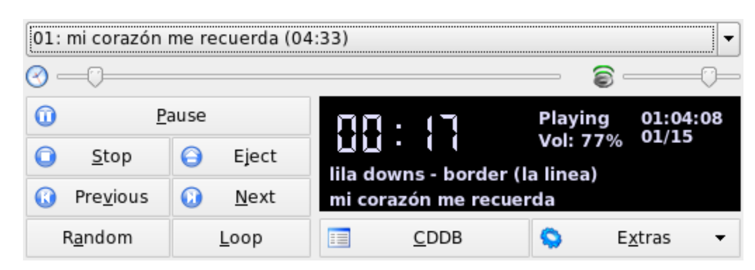
IMPORTANT: CDDA et lecture analogique de CD

Il existe deux manières de lire des CD audio. Les lecteurs de CD et de DVD qui peuvent lire des CD analogiques lisent les données audio, puis les envoient au périphérique de sortie. Certains lecteurs externes, connectés via PCMCIA, FireWire ou USB doivent recourir à CDDA (Compact Disk Digital Audio - audio numérique CD) pour extraire les données audio, puis les lire au format PCM numérique. Les lecteurs présentés ici ne prennent pas en charge CDDA. Si vous devez prendre en charge CDDA, utilisez XMMS.

7.3.1 KsCD : lecteur de CD audio

KsCD est un lecteur de CD audio facile à utiliser. Il s'intègre à la barre des tâches KDE et peut être configuré afin de démarrer la lecture automatiquement lors de l'insertion d'un CD. Pour accéder au menu de configuration, sélectionnez *Extras* → *Configure KsCD (Configurer KsCD)*. Téléchargez les informations d'album et de piste à partir d'un serveur CDDB sur Internet, si KsCD est configuré pour cela. Vous pouvez également télécharger des informations vers le serveur CDDB pour les partager avec d'autres. Pour l'extraction et le partage d'informations, utilisez la boîte de dialogue *CDDB*.

Figure 7.6 *L'interface utilisateur de KsCD*



7.3.2 L'applet Lecteur de CDs audio de GNOME

Il s'agit d'une simple applet intégrée au tableau de bord GNOME. A l'aide de l'icône des outils, configurez son comportement et sélectionnez un thème. Vous contrôlez la lecture avec les boutons (en bas de la fenêtre du lecteur) ou via le menu contextuel (cliquez avec le bouton droit de la souris sur l'icône du tableau de bord ou dans la fenêtre du lecteur).

7.3.3 Compression des données audio

La compression audio peut être gérée par divers outils. Les sections suivantes décrivent l'encodage et la lecture de données audio via la ligne de commande, ainsi que certaines applications graphiques qui offrent des fonctions de compression audio.

Outils de ligne de commande pour l'encodage et la lecture des données audio

Ogg Vorbis (paquetage `vorbis-tools`) est un format de compression audio libre, désormais pris en charge par la plupart des lecteurs audio et même des baladeurs MP3. La page Web de ce projet est `http://www.xiph.org/ogg/vorbis`.

SUSE Linux est livré avec plusieurs outils qui prennent en charge Ogg Vorbis. `oggenc` est un outil de ligne de commande qui encode les fichiers WAV au format Ogg. Il suffit d'exécuter `oggenc` *`nom_fichier.wav`* pour convertir au format Ogg Vorbis un fichier `.wav` spécifique. L'option `-h` affiche une présentation des autres paramètres. Oggenc prend en charge l'encodage avec un débit binaire variable. Ainsi, il est possible d'obtenir un degré de compression encore meilleur. Au lieu du débit binaire, vous pouvez spécifier la qualité souhaitée (paramètre `-q`) ; l'option `-b` détermine le débit binaire moyen, alors que `-m` et `-M` spécifient le débit binaire minimum et maximum.

ogg123 est un lecteur Ogg de ligne de commande. Vous le démarrez avec une commande comme `ogg123` *`ma_chanson.ogg`* .

Compression de données audio avec Grip

Grip est un lecteur de CD extracteur (RIP) GNOME (consultez la Figure 7.7, « Extraction (RIP) de CD audio avec Grip » (p. 133)). Vous contrôlez entièrement la fonction de lecteur de CD avec les boutons, en bas de la fenêtre. Pour contrôler les fonctions d'extraction (RIP) et d'encodage, vous utilisez les onglets situés en haut de la fenêtre. Pour afficher et modifier des informations sur l'album et ses pistes, ou pour sélectionner les pistes à extraire (RIP), ouvrez l'onglet *Tracks* (Pistes). Sélectionnez une piste en cliquant sur la case à côté de son titre. Pour modifier les informations relatives à un morceau, cliquez sur *Toggle disc editor* (Activer/Désactiver l'éditeur de disque), puis soumettez vos modifications. L'onglet *Rip* sélectionne le mode d'extraction (RIP) le mieux adapté et contrôle le processus. L'onglet *Config* permet d'accéder à la configuration complète de Grip. Utilisez l'option *Status* (État) pour contrôler l'état de l'application.

***Figure 7.7** Extraction (RIP) de CD audio avec Grip*

Compression de données audio avec KAudioCreator

KAudioCreator est une application d'extraction (RIP) de CD légère (consultez la Figure 7.8, « Extraction (RIP) de CD audio avec KAudioCreator » (p. 134)). Une fois démarrée, elle répertorie les morceaux présents sur le CD, dans l'onglet *CD Tracks* (Pistes du CD). Sélectionnez les pistes à extraire (RIP) et à encoder. Pour modifier les informations relatives à la piste, utilisez l'*éditeur d'album*, accessible via le menu *File (Fichier)* → *Edit Album (Modifier l'album)*. Sinon, démarrez simplement l'extraction (RIP) et l'encodage avec *File (Fichier)* → *Rip Selection (Extraire la sélection)*. Observez la progression de ces opérations dans l'onglet *Jobs* (Travaux). Selon sa configuration, KAudioCreator génère également des fichiers de liste de lecture qui peuvent être utilisés par des lecteurs comme amaroK ou XMMS.

Figure 7.8 *Extraction (RIP) de CD audio avec KAudioCreator*

Compression de CD audio avec Konqueror

Avant de lancer l'extraction (RIP) proprement dite avec Konqueror, configurez la gestion des CD audio et de l'encodeur Ogg Vorbis dans le centre de contrôle KDE. Sélectionnez *Sound & Multimedia (Son et multimédia)* → *Audio CDs (CD audio)*. Le module de

configuration comporte trois onglets : *General* (Général), *Names* (Noms) et *Ogg Vorbis Encoder* (Encodeur Ogg Vorbis). Normalement, tout lecteur de CD adapté est automatiquement détecté. Ne modifiez pas ce comportement par défaut, à moins que la détection automatique ait échoué et que vous soyez contraint de configurer manuellement le lecteur de CD. La correction des erreurs et la priorité d'encodage sont également configurées ici. L'onglet *Ogg Vorbis Encoder* (Encodeur Ogg Vorbis) détermine la qualité de l'encodage. Pour configurer la consultation en ligne des informations relatives à un album, une piste ou un artiste correspondant à vos données audio extraites (RIP), sélectionnez *Add Track Information* (Ajouter des informations sur la piste).

Démarrez le processus d'extraction (RIP) en insérant le CD dans le lecteur de CD et en entrant `audiocd:/` dans la barre d'*adresse*. Konqueror affiche alors les pistes du CD et quelques dossiers (consultez la Figure 7.9, « Extraction (RIP) de données audio avec Konqueror » (p. 135)).

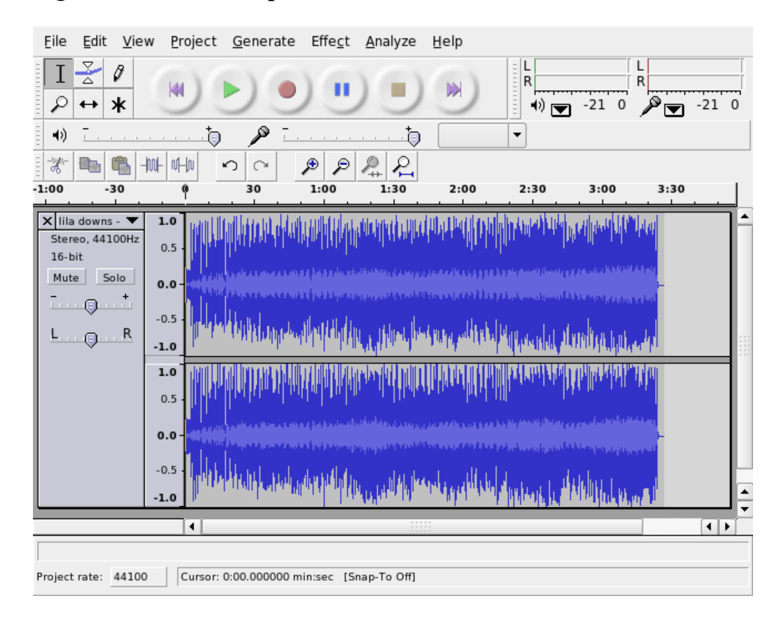
Figure 7.9 *Extraction (RIP) de données audio avec Konqueror*

Pour conserver des données audio non compressées sur votre disque, il suffit de sélectionner les fichiers `.wav` et de les faire glisser vers une autre fenêtre Konqueror afin de les copier vers leur destination finale. Pour démarrer l'encodage Ogg Vorbis, faites glisser le dossier `Ogg Vorbis` vers une autre fenêtre Konqueror. L'encodage démarre dès que vous déposez le dossier Ogg Vorbis à son emplacement de destination.

7.4 Enregistrement sur disque dur avec Audacity

Audacity (paquetage `audacity`) permet d'enregistrer et de modifier des fichiers audio. L'opération est appelée « enregistrement sur le disque dur ». Lorsque vous démarrez le programme pour la première fois, sélectionnez la langue. Vous pouvez modifier la langue ultérieurement, via le menu *File (Fichier) → Preferences (Préférences) → Interface*. Le changement de langue est appliqué au démarrage suivant du programme.

Figure 7.10 *Vue spectrale des données audio*



7.4.1 Enregistrement de fichiers WAV et importation de fichiers

Cliquez sur le bouton d'enregistrement rouge pour créer une piste stéréo vide et démarrer l'enregistrement. Pour modifier les paramètres standard, effectuez les réglages souhaités sous *File (Fichier) → Preferences (Préférences)*. Les *entrées/sorties audio* et la *qualité* sont des critères importants pour l'enregistrement. Même si les pistes

existent déjà, d'autres sont créées lorsque vous cliquez sur le bouton d'enregistrement. Cela peut prêter à confusion au début, car ces pistes n'apparaissent pas dans la fenêtre affichée à sa taille standard.

Pour importer des fichiers audio, sélectionnez *Project (Projet) → Import Audio (Importer audio)*. Le programme prend en charge le format WAV et le format compressé Ogg Vorbis. Pour plus d'informations sur ce format, consultez la Section 7.3.3, « Compression des données audio » (p. 132).

7.4.2 Modification de fichiers audio

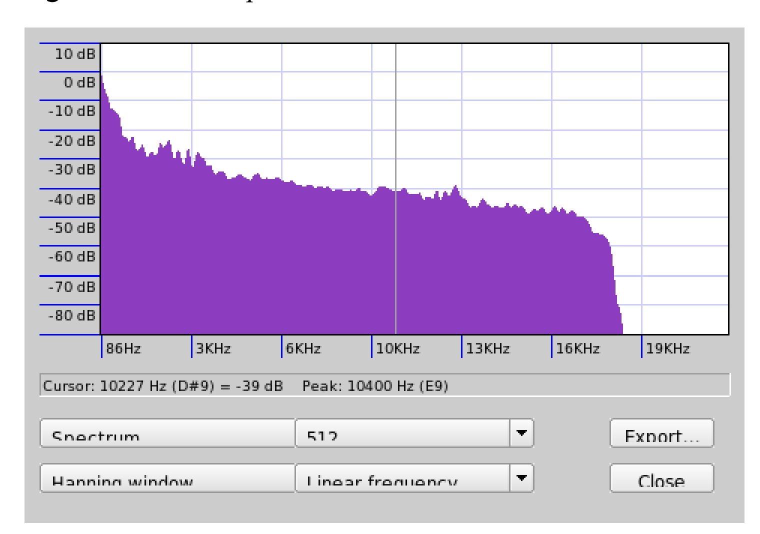
Ouvrez le menu *AudioTrack*, à gauche de la piste. Ce menu comporte diverses options d'affichage et présente les opérations de modification de base. Pour renommer une piste, sélectionnez *Name* (Nom), puis saisissez un nouveau nom. Les différents modes d'affichage offerts par Audacity incluent notamment les vues *Waveform* (Forme d'onde), *Waveform (dB)* (Forme d'onde (dB)), *Spectrum* (Spectre) et *Pitch* (Hauteur). Choisissez ce qui correspond le mieux à vos besoins. Si vous souhaitez modifier séparément chaque canal d'une piste stéréo, sélectionnez *Split Track* (Fractionner la piste). Chaque canal sera considéré comme une piste distincte. Pour chaque piste, définissez le *format d'échantillonnage* (en bit) et le *taux d'échantillonnage* (en Hz).

Pour pouvoir utiliser la plupart des outils du menu *Edit* (Édition), vous devez d'abord sélectionner le canal et le segment de piste à modifier. Une fois la sélection effectuée, vous pouvez lui appliquer toutes sortes de modifications et d'effets.

Selon le type de fichier choisi, vous disposez de divers formats d'affichage des segments sélectionnés, sous *View (Affichage) → Set Selection Format (Définir le format de sélection)*. La fonction *Set Snap-To Mode* (Activer le mode magnétique) permet l'adaptation automatique des limites de segment au format d'affichage choisi. Par exemple, si vous sélectionnez *PAL frames* (Trames PAL) comme format d'affichage et que vous activez *Snap-To*, les limites de segment seront toujours sélectionnées selon un multiple du nombre de trames.

Tous les outils de modification sont accompagnés d'info-bulles et devraient donc être faciles à utiliser. La fonction d'*historique pour l'annulation*, sous *View (Affichage) → History (Historique)*, est très utile pour afficher les étapes de modification récentes et les annuler en cliquant dessus dans la liste. Utilisez l'option *Discard* (Rejeter) avec prudence car elle efface les étapes de modifications de la liste. Une fois effacées, ces étapes ne peuvent plus être annulées.

Figure 7.11 *Le spectre*



La fonction intégrée d'analyse de spectre vous aide à détecter rapidement les bruits de fond. Affichez le spectre du segment sélectionné, avec *View (Affichage)* → *Plot Spectrum (Tracer le spectre)*. Sélectionnez une échelle de fréquence logarithmique en octaves à l'aide de l'option *Log frequency* (Fréquence logarithmique). Si vous déplacez le pointeur de la souris dans le spectre, les fréquences de pics sont automatiquement affichées, ainsi que les notes correspondantes.

Supprimez les fréquences indésirables, avec *Effect (Effet)* → *FFT Filter (Filtre FFT)*. Si vous activez un filtre, il peut être nécessaire de réajuster l'amplitude du signal, avec l'option *Amplify* (Amplifier). Vous pouvez également utiliser *Amplify* pour vérifier l'amplitude. Par défaut la *nouvelle amplitude de pic* est définie sur 0,0 dB. Cette valeur représente l'amplitude maximum possible dans le format audio sélectionné. L'option *Amplification* affiche la valeur nécessaire pour amplifier le segment sélectionné jusqu'à son amplitude maximum. Une valeur négative indique une suramplification.

7.4.3 Enregistrement et exportation

Pour enregistrer un projet entier, sélectionnez *File (Fichier)* → *Save Project (Enregistrer le projet)* ou *Save Project As* (Enregistrer le projet sous). Cela génère un fichier XML d'extension `.aup`, qui décrit le projet. Les données audio réelles sont enregistrées dans un répertoire qui porte le nom du projet, suivi de `_data`.

Vous pouvez également exporter le projet entier (ou le segment sélectionné) sous la forme d'un fichier WAV stéréo. Pour exporter le projet au format Ogg Vorbis, consultez la Section 7.3.3, « Compression des données audio » (p. 132).

7.5 Lecture et enregistrement directs de fichiers WAV

Les fonctions `arecord` et `aplay` du paquetage `alsa` fournissent une interface simple et adaptable pour les périphériques PCM. `arecord` et `aplay` permettent d'enregistrer et de lire des données audio dans divers formats, dont WAV. La commande `arecord -d 10 -f cd -t wav mysong.wav` enregistre un fichier WAV de 10 secondes en qualité CD (16 bits, 44,1 kHz). Vous affichez la liste de toutes les options d'`arecord` et d'`aplay` en les exécutant avec l'option `--help`.

qaRecord (paquetage `kalsatools`) est un programme d'enregistrement simple doté d'une interface graphique et d'un affichage des niveaux. Comme ce programme utilise une mémoire tampon interne d'environ 1 Mo (configurable avec `--buffersize`), il permet de procéder à des enregistrements continus même sur du matériel lent, en particulier s'il est exécuté avec une priorité Temps réel. Au cours de l'enregistrement, la taille de la mémoire tampon actuellement utilisée est affichée dans la ligne d'état, sous *Buffer* (Tampon) et la taille maximum de mémoire tampon employée jusque-là pour cet enregistrement est affichée sous *Peak* (Pic).

Figure 7.12 *QARecord : un programme simple d'enregistrement sur disque dur*

TV, Vidéo, Radio et Webcam

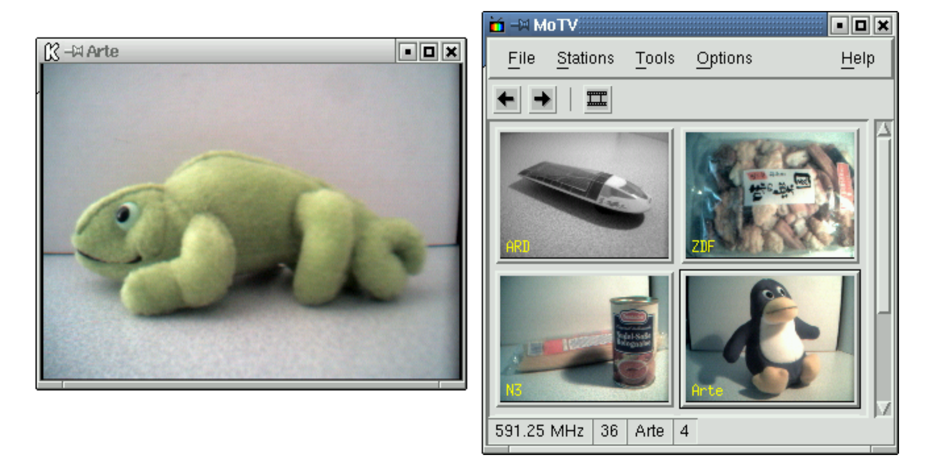
8

Ce chapitre présente quelques applications de base Linux dédiées à la vidéo, à la radio et aux webcams. Apprenez à configurer et à utiliser motv pour regarder la télévision analogique, utiliser une webcam et parcourir du vidéotexte. Utilisez xawtv4 pour la diffusion vidéo numérique. Les webcams peuvent être contrôlées avec gqcam. Pour accéder à des données EPG, utilisez nxtvepg ou xawtv4.

8.1 Regarder la télévision avec motv

motv est le successeur amélioré de xawtv. Il intègre toutes les fonctions essentielles dans l'interface utilisateur. Démarrez l'application en sélectionnant *Multimedia (Multimédia) → Video (Vidéo) → motv*. Vous pouvez également taper `motv` à la ligne de commande. Au départ, au démarrage de l'application, seule une fenêtre TV apparaît. Cliquez dessus avec le bouton droit pour ouvrir une fenêtre de menus.

Figure 8.1 *L'application TV motv*



8.1.1 Source vidéo et recherche de réseau

Sous *Settings (Paramètres)* → *Input (Entrée)*, sélectionnez la source vidéo. Si vous sélectionnez *Télévision*, configurez le réseau de diffusion avant de démarrer l'application. Ceci se fait automatiquement lors de la recherche de réseau, une option à laquelle vous pouvez également accéder à partir du menu *Paramètres*. Si vous cliquez sur *Enregistrer les paramètres*, le réseau trouvé est inséré dans le fichier `.xawtv` de votre dossier personnel et vous sera proposé lors du prochain démarrage de l'application.

ASTUCE: Sélection de canaux

Si vous ne voulez pas parcourir tous les canaux disponibles, trouvez le canal suivant au moyen de la combinaison de touches Ctrl + ↑. Si nécessaire, réglez ensuite la fréquence de diffusion, avec ← ou →.

8.1.2 Récupération de données audio

La sortie audio de la carte TV est connectée à l'entrée ligne de votre carte son, aux haut-parleurs ou à un amplificateur. Certaines cartes TV peuvent modifier le volume de la sortie audio. Le volume peut être réglé au moyen des glissières qui apparaissent lorsque

vous cliquez sur *Paramètres* → *Glissière*. Cette fenêtre propose également des glissières pour la luminosité, le contraste et les couleurs.

Pour utiliser votre carte son pour la sortie audio, vérifiez les paramètres de mixage au moyen de gamix (consultez la Section 7.1, « Mixeurs » (p. 119)). Pour les cartes son qui respectent les spécifications AC97, réglez *Input-MUX* (Entrée-Mux) sur *Ligne*. Vous pouvez ensuite régler le volume au moyen des glissières *Maître* et *Ligne*

8.1.3 Dimensions de l'écran et mode Plein écran

La plupart des images télévisées ont un rapport hauteur-largeur de 4:3. Ces proportions peuvent être définies dans *Outils* → *Screen Dimensions* (Dimensions de l'écran). Si la valeur (par défaut) de *4:3* est sélectionnée, les dimensions de l'écran sont automatiquement conservées, même lorsque la taille d'affichage change.

La touche F ou l'option *Outils* → *Plein Écran* permettent de passer en mode plein écran. Si l'image TV n'occupe pas tout le moniteur en mode plein écran, un réglage plus poussé est nécessaire. Beaucoup de cartes graphiques sont capables d'élargir l'image TV en mode plein écran afin qu'elle occupe tout le moniteur et ce, sans changer de mode graphique. Si votre carte ne prend pas en charge cette fonction, vous devez choisir 640x480 comme mode graphique pour le mode plein écran. Créez la configuration associée sous *Settings (Paramètres)* → *Configuration*. Après avoir redémarré motv, le mode moniteur change aussi si vous choisissez le mode plein écran.

ASTUCE: Stockage de la configuration dans le fichier .xawtv

Le fichier `.xawtv` est créé automatiquement et mis à jour lorsque vous cliquez sur *Paramètres* → *Enregistrer les paramètres*. Ici, les émetteurs sont enregistrés en même temps que la configuration. Pour plus d'informations sur le fichier de configuration, reportez-vous à la section du manuel qui porte sur `xawtvrc`.

8.1.4 Le menu Lanceur

Le menu du programme de lancement vous permet d'exécuter d'autres applications en combinaison avec motv. Par exemple, démarrez le mixeur audio gamix et l'application

de vidéotexte alevt, à l'aide d'un raccourci clavier. Les applications à lancer à partir de motv doivent figurer dans le fichier `.xawtv`. comme ceci :

```
[launch] Gamix = Ctrl+G, gamix AleVT = Ctrl+A, alevt
```

Le nom de l'application doit être suivi du raccourci clavier, puis de la commande utilisée pour lancer l'application. Pour lancer les applications qui figurent sous [lanceur], utilisez le menu *Outil*.

8.2 Prise en charge du vidéotexte

L'outil alevt vous permet de consulter des pages de vidéotexte. Démarrez l'application avec *Multimedia (Multimédia)* → *Video (Vidéo)* → *alevt* ou en entrant `alevt` sur la ligne de commande.

L'application enregistre toutes les pages de la station sélectionnée que vous venez d'activer avec motv. Parcourez les pages en tapant le numéro de page souhaité ou en cliquant sur un numéro de page. Passez d'une page à l'autre en cliquant sur les boutons << ou >>, situés dans la marge de la fenêtre inférieure.

Les versions récentes de motv (et de son successeur xawtv4) intègrent leurs propres applications d'affichage de vidéotexte : mtt (motv) et mtt4 (xawtv4). mtt4 prend même en charge les cartes DVB.

8.3 Webcams et motv

Si votre webcam est déjà prise en charge par Linux, accédez-y avec motv. Vous trouverez une synthèse des périphériques USB pris en charge sur http://www.linux-usb.org. Si vous avez déjà utilisé motv pour accéder à votre carte TV (avant d'accéder à la webcam), le pilote bttv est déjà chargé. Le pilote de la webcam est chargé automatiquement lorsque vous connectez celle-ci au port USB. Démarrez motv sur la ligne de commande avec le paramètre `-c /dev/video1` afin d'accéder à la webcam. Accédez à la carte TV en tapant `motv -c /dev/video0`.

Si vous connectez la webcam au port USB avant le chargement automatique du pilote bttv (par exemple, en démarrant une application TV), la commande `/dev/video0` est réservée à la webcam. Dans ce cas, si vous démarrez motv avec le paramètre `-c /dev/video1` afin d'accéder à la carte TV, vous risquez d'obtenir un

message d'erreur, parce que le pilote bttv n'a pas été chargé automatiquement. Pour résoudre ce problème, chargez le pilote séparément au moyen du paramètre `modprobe bttv` en tant qu'utilisateur `root`. Le paramètre `motv -hwscan` affiche un aperçu des périphériques vidéo configurables sur votre système.

8.4 nxtvepg : le magasine télé de votre PC

Certains émetteurs transmettent un signal EPG (Electronic Program Guide, guide électronique des programmes) en même temps que leur signal vidéotexte. Le programme nxtvepg vous permet de consulter facilement ce guide électronique. Cependant, pour pouvoir en profiter, votre carte TV doit être prise en charge par le pilote bttv et être capable de recevoir un des canaux diffusés avec un signal EPG.

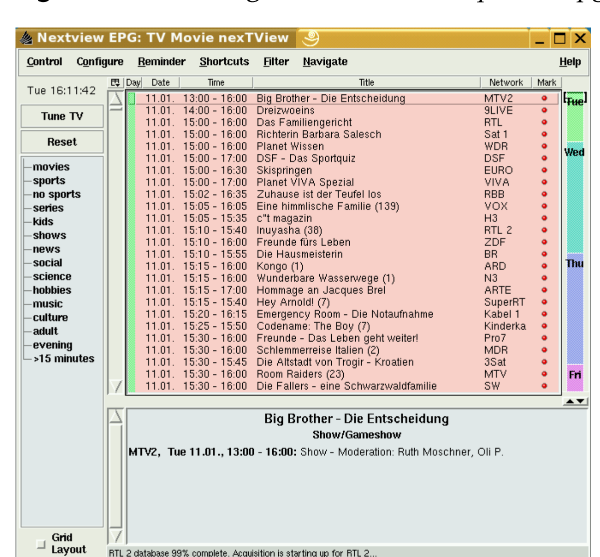
L'application nxtvepg classe les émetteurs par canal et par sujet (comme *cinéma* et *sports*), et les filtre en fonction de certains critères (*Live* (En direct), *Stereo* (En stéréo) ou *Subtitle* (Sous-titré)). Démarrez l'application avec *Multimedia (Multimédia)* → *Video (Vidéo)* → *nxtvepg* ou en entrant `nxtvepg` sur la ligne de commande.

8.4.1 Importation de la base de données EPG

Pour configurer et mettre à jour la base de données de programmes via le signal EPG, réglez le tuner de votre carte TV sur une station qui émet un signal EPG. Utilisez pour ce faire une application TV, comme motv ou nxtvepg. Le tuner est accessible à une seule application à la fois.

Si vous définissez un émetteur EPG dans motv, nxtvepg démarre immédiatement l'importation de la liste de programmes TV actuelle. La progression est affichée.

Figure 8.2 *Le magazine télé électronique nxtvepg*



Si vous n'avez pas encore démarré votre application TV, laissez nxtvepg rechercher des émetteurs EPG. Pour ce faire, sélectionnez *Configurer* → *Provider scan* (Recherche de fournisseurs). L'option *Use .xatv* (Utiliser .xatv) est activée par défaut. Cela signifie que nxtvepg va accéder aux émetteurs enregistrés dans ce fichier.

ASTUCE: Dépannage

En cas de problème, vérifiez que la bonne source vidéo a été choisie dans *TV card input* (Entrée de la carte TV).

Sélectionnez un des fournisseurs EPG trouvés dans *Configurer* → *Select Provider* (Sélectionner le fournisseur). L'option *Configurer* → *Merge Providers* (Fusionner les fournisseurs) va même jusqu'à créer des associations flexibles entre les différentes bases de données des fournisseurs.

8.4.2 Tri des programmes

nxtvepg est doté d'une fonction de filtre très pratique qui permet de gérer les offres télévisuelles les plus complètes. Sélectionnez *Configurer* → *Show networks* (Afficher les réseaux) pour activer le choix de réseaux. Le menu *Filtre* propose une multitude de

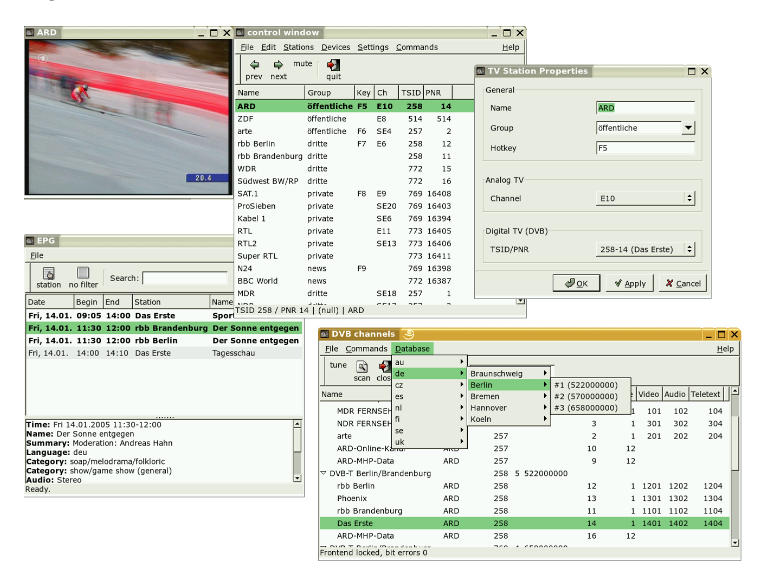
fonctions de filtrage. Cliquez avec le bouton droit sur la liste de programmes pour ouvrir un menu de filtrage spécial dans lequel vous pouvez activer les fonctions de filtrage contextuel.

Le menu *Navigate* (Naviguer) est particulièrement intéressant. Ce menu est compilé directement à partir des données EPG. Il apparaît dans la langue du réseau.

8.5 Regarder des émissions vidéo numériques avec xawtv4

Une fois votre matériel correctement configuré avec YaST, démarrez xawtv4 à partir du menu principal (*Multimedia (Multimédia)* → *Video (Vidéo)* → *xawtv4*). Avant de pouvoir regarder vos émissions favorites, créez une base de données des stations DVB.

***Figure 8.3** Exécution de xawtv4*



Cliquez avec le bouton droit de la souris sur la fenêtre de démarrage pour ouvrir la fenêtre de contrôle (consultez la Figure 8.3, « Exécution de xawtv4 » (p. 147)). Démarrez une recherche des stations DVB disponibles en sélectionnant *Edit (Édition)* → *Scan DVB (Rechercher DBV)*. Une fenêtre de recherche de canaux et d'exploration apparaît. Sélectionnez un bouquet pour préparer la recherche. Cette opération peut être effectuée

manuellement via *Commands (Commandes)* → *Tune manually (Réglage manuel)* si vous connaissez déjà les paramètres de réglage du bouquet, ou si vous les obtenez à partir d'une base de données intégrée xawtv4 via *Database (Base de données)* → *_country_* → *_channel number_* (remplacez `_country_` et `_channel_number_` par votre pays et le numéro de chaîne voulu).

Dès que la recherche est configurée, les premières données sont affichées dans la fenêtre de navigation. Lancez une recherche complète de toutes les stations disponibles, avec *Command (Commande)* → *Full Scan (Balayage complet)*. Pendant la recherche, vous pouvez sélectionner vos stations favorites et les ajouter à la liste des stations : il suffit de les faire glisser vers la fenêtre de contrôle. Quittez la recherche de chaînes et sélectionnez l'une des chaînes pour commencer à regarder l'émission.

ASTUCE: Modification de la liste des stations

À l'aide de raccourcis clavier, vous pouvez contrôler la sélection des chaînes avec le clavier. Pour définir un raccourci clavier pour une station de votre liste, sélectionnez cette station, cliquez sur *Edit (Édition)* → *Edit Station (Modifier la station)*. La boîte de dialogue appelée *TV Station Properties (Propriétés de la station TV)* s'ouvre. Entrez le raccourci clavier, puis quittez la boîte de dialogue en cliquant sur *OK*. Cette boîte de dialogue permet également de définir des sous-menus contenant des groupes de chaînes (comme « informations » ou « privé »).

Le paquetage logiciel xawtv4 contient plusieurs autres applications multimédias autonomes très utiles :

pia4
: Lecteur vidéo léger contrôlé par ligne de commande, qui peut servir à lire les flux vidéo enregistrés par xawtv4.

mtt4
: Navigateur de vidéotexte (consultez la Figure 8.4, « Le navigateur de vidéotexte mtt4 » (p. 149)).

Figure 8.4 Le navigateur de vidéotexte mtt4



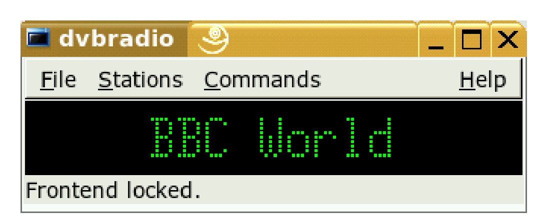
alexplore

Application autonome de recherche de chaînes DVB. Ses fonctionnalités sont intégrées à xawtv4.

dvbradio

Émetteur radio DVB. Permet d'écouter les flux radio DVB-S une fois la recherche de stations initiale terminée (consultez la Figure 8.5, « dbvradio » (p. 149)).

Figure 8.5 dbvradio



dvbrowse

Explorateur EPG. Permet d'obtenir des informations EPG une fois la recherche de stations initiale terminée.

9 K3b – Gravure de CD ou de DVD

K3b est un programme complet de gravure de DVD et de CD audio et de données. Démarrez le programme à partir du menu principal ou en tapant la commande `k3b`. Dans les sections suivantes, vous allez apprendre à lancer un processus de gravure classique qui vous permettra d'obtenir votre premier CD ou DVD Linux.

9.1 Création d'un CD de données

Pour créer un CD de données, cliquez sur *File (Fichier)* → *New Project (Nouveau projet)* → *New Data Project (Nouveau projet de données)*. La vue de projet apparaît dans la partie inférieure de la fenêtre (voir la Figure 9.1, « Création d'un nouveau CD de données » (p. 152)). Pour ajouter un répertoire ou un fichier au projet, sélectionnez-le dans votre dossier personnel et déplacez-le dans le dossier du projet au moyen d'un simple glisser-déposer. Enregistrez le projet sous le nom de votre choix en sélectionnant *File (Fichier)* → *Save as (Enregistrer sous)*.

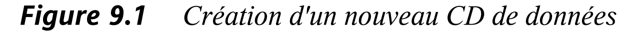
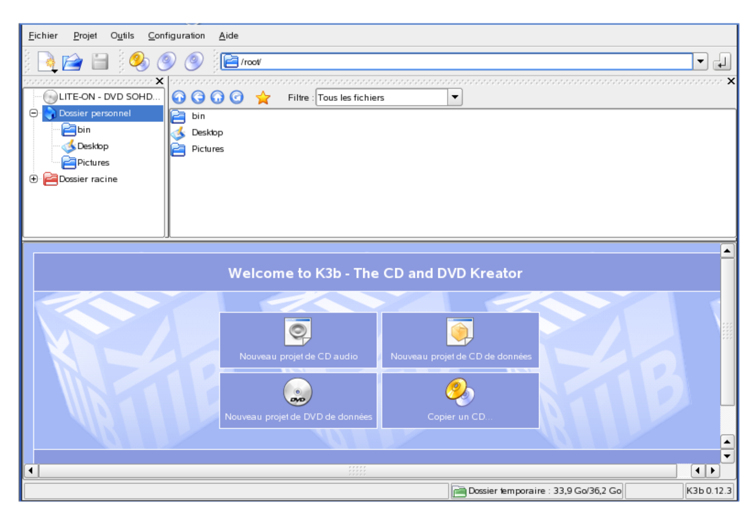
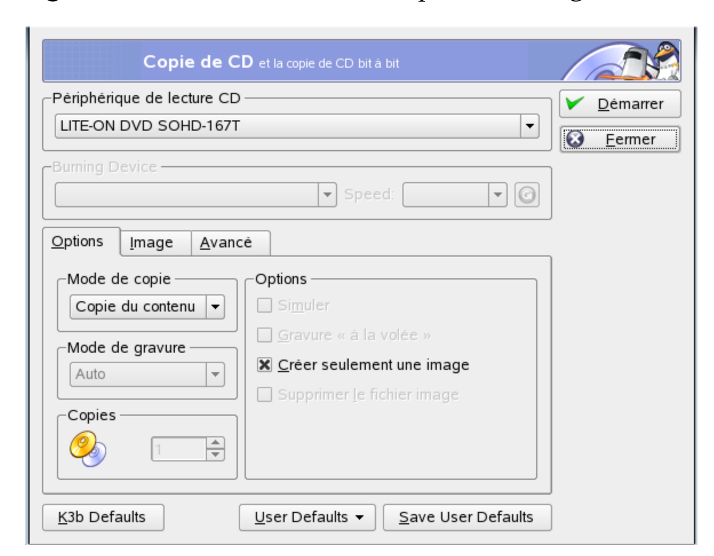


Figure 9.1 *Création d'un nouveau CD de données*



Sélectionnez ensuite *Burn* (Graver) dans la barre d'outils, ou appuyez sur les touches Ctrl + B. Une boîte de dialogue composée de six onglets d'options de gravure apparaît. (voir Figure 9.2, « Personnalisation du processus de gravure » (p. 152)).

Figure 9.2 *Personnalisation du processus de gravure*



L'onglet *Writing* (Écriture) contient différents paramètres relatifs au périphérique de gravure, à la vitesse et aux options de gravure. Voici les options possibles :

Burning Device (Périphérique de gravure)

Le graveur détecté est affiché dans ce menu contextuel. Vous pouvez également choisir ici la vitesse de gravure.

AVERTISSEMENT: Sélectionnez la vitesse de gravure avec soin.

Vous sélectionnez normalement l'option *Auto* (Automatique), qui choisit la vitesse de gravure maximum. Toutefois, si vous choisissez une valeur supérieure et que votre système n'a pas la capacité de transmettre les données suffisamment rapidement, vous risquez de perdre des données à cause d'un dépassement négatif du tampon.

Writing Mode (Mode d'écriture)

Cette option détermine la manière dont le laser grave le CD. En mode DAO (disk at once, disque à disque), le laser n'est pas désactivé pendant la gravure du CD. Ce mode est recommandé pour la création de CD audio. Sachez toutefois qu'il n'est pas pris en charge par tous les graveurs. En mode TAO (track at once, piste à piste), un processus de gravure séparé est utilisé pour chacune des pistes. L'utilisation du mode RAW est peu fréquente en raison de l'absence de corrections des données. La meilleure solution consiste à choisir l'option *Auto* (Automatique) car elle permet à K3b d'utiliser les paramètres les plus adéquats.

Simuler

Cette fonction permet de vérifier si votre système accepte la vitesse de gravure sélectionnée. La gravure se fait sans laser, afin de tester le système.

On the Fly (À la volée)

Cette fonction permet de graver les données sélectionnées sans créer de fichier d'image au préalable (son utilisation est à proscrire sur les systèmes moins performants). Un fichier d'image, également connu sous le nom d'image ISO, est un fichier contenant toutes les données qui vont être gravées telles quelles sur le CD.

Only Create Image (Créer une image uniquement)

Cette option crée un fichier d'image. Spécifiez le chemin d'accès de ce fichier sous *Fichier temporaire*. Ce fichier d'image est stocké en mémoire afin de pouvoir être gravé sur CD ultérieurement. Pour ce faire, utilisez *Tools (Outils) → CD → Burn*

CD Image (Graver l'image du CD). Si cette option est utilisée, toutes les autres options de cette section sont désactivées.

Remove Image (Supprimer l'image)
Cette option supprime du disque le fichier image temporaire une fois la gravure terminée.

Verify Written Data (Vérifier les données gravées)
Cette option vérifie l'intégrité des données gravées en comparant les sommes MD5 des données d'origine et les données gravées.

L'onglet *Image* n'est accessible que si l'option *Only create image* (Créer une image uniquement) de l'onglet précédent est sélectionnée. Si vous y avez accès, vous pouvez déterminer le fichier dans lequel les données ISO sont écrites.

L'onglet *Settings* (Configuration) propose deux options : *Datatrack Mode* (Mode pistes de données) et *Multisession Mode* (Mode multisession). L'option *Datatrack Mode* permet de configurer le mode de gravure des pistes de données. Il est recommandé, en général, d'utiliser le paramètre *Auto* (Automatique). L'option *Multisession Mode* permet d'ajouter des données à un CD déjà gravé mais pas finalisé.

Dans l'onglet *Volume Desc* (Description volume), entrez des informations générales qui serviront à identifier ce projet de données particulier, son auteur et son éditeur, ainsi que l'application et le système d'exploitation utilisés pour la création de ce projet.

Sous *Système de fichiers*, définissez les paramètres relatifs au système de fichiers sur le CD (RockRidge, Joliet, UDF). Choisissez aussi la manière dont sont traités les liens symboliques, les autorisations de fichier et les blancs. L'onglet *Advanced* (Avancé) contient des paramètres supplémentaires réservés aux utilisateurs expérimentés.

Une fois les paramètres définis selon vos besoins, lancez le processus de gravure réel à l'aide de l'option *Burn* (Graver). Vous pouvez également enregistrer ces paramètres en vue d'une utilisation ou d'une modification ultérieure en cliquant sur *Save* (Enregistrer).

9.2 Création d'un CD audio

À la base, rien ne différencie véritablement la création d'un CD audio de la création d'un CD de données. Pour commencer, sélectionnez *Fichier → New Audio Project*

(Nouveau projet audio). Glissez et déposez les pistes audio de votre choix dans le dossier du projet. Les données audio doivent être au format WAV ou Ogg Vorbis. Pour modifier l'ordre des pistes, déplacez-les vers le haut ou vers le bas dans le dossier du projet.

À l'aide de l'option (Texte CD), vous pouvez ajouter certaines informations texte sur un CD, telles que le titre du CD, le nom de l'artiste et le nom de chaque piste. Les lecteurs CD qui prennent en charge cette fonctionnalité peuvent lire et afficher ces informations. Pour ajouter des informations texte à vos pistes audio, commencez par sélectionner la piste souhaitée. Cliquez dessus avec le bouton droit, puis sélectionnez *Properties* (Propriétés). Une nouvelle fenêtre apparaît ; entrez-y les informations souhaitées.

La boîte de dialogue de gravure d'un CD audio ressemble fortement à celle de la création d'un CD de données. Toutefois, le choix de l'option *Disc at once* (Mode Disc-At-Once (DAO)) ou du mode *Track at once* (Mode Track-At-Once) est plus déterminant. En effet, le mode *Track at once* insère une pause de deux secondes après chaque piste.

ASTUCE: Préservation de l'intégrité des données

Lorsque vous gravez des CD audio, choisissez une vitesse de gravure faible pour réduire les risques d'erreurs de gravure.

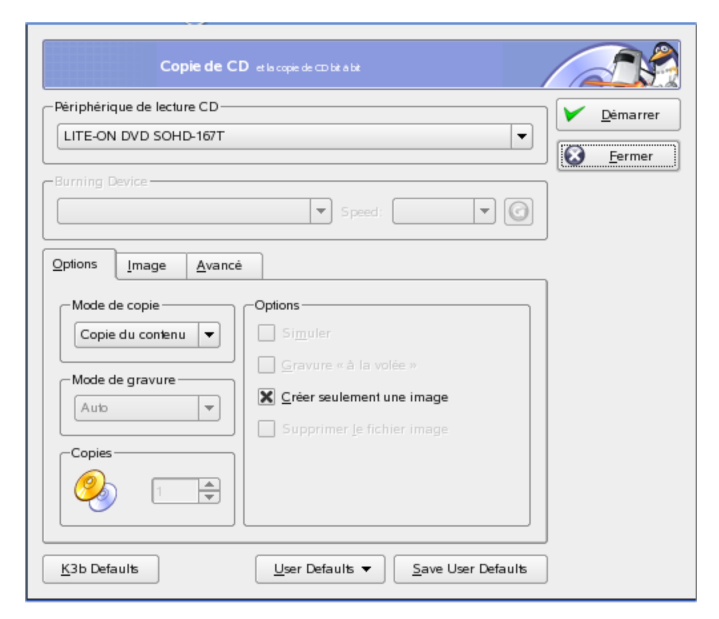
Une fois les paramètres définis selon vos besoins, lancez le processus de gravure réel à l'aide de l'option *Burn* (Graver). Vous pouvez également enregistrer ces paramètres en vue d'une utilisation ou d'une modification ultérieure en cliquant sur *Save* (Enregistrer).

9.3 Copie d'un CD ou d'un DVD

Sélectionnez *Tools (Outils) → Copy CD (Copier un CD)* ou *Tools (Outils) → Copy DVD (Copier un DVD)*, en fonction du support utilisé. Dans la boîte de dialogue qui apparaît, réglez les paramètres relatifs au périphérique de lecture et de gravure (voir la Figure 9.3, « Copie d'un CD » (p. 156)). Les options d'écriture mentionnées ci-dessus sont disponibles ici également. Une fonction supplémentaire permet de créer plusieurs copies d'un même CD ou DVD.



Figure 9.3 Copie d'un CD



Cochez la case *On the fly* (À la volée) pour graver le CD dès qu'il a été lu, ou sélectionnez *Only create image* (Créer une image uniquement) pour créer une image à l'emplacement indiqué dans *Temp Directory (Répertoire temp.)* → *Write image file to (Écrire le fichier d'image dans)* et graver l'image ultérieurement.

9.4 Gravure d'images ISO

Si vous disposez déjà d'une image ISO, sélectionnez *Tools (Outils)* → *CD* → *Burn CD image (Graver une image ISO)*. Dans la fenêtre qui s'ouvre, indiquez l'emplacement de l'image à graver dans *Image to Burn* (Image à graver). K3b établit une somme de contrôle et l'affiche dans *MD5 Sum* (Somme de contrôle MD5). Si le fichier ISO provient d'Internet, cette somme indique si le téléchargement avait réussi.

Utilisez les onglets *Options* et *Avancé* pour définir vos préférences. Pour graver le CD, cliquez sur *Start* (Démarrer).

9.5 Création d'un CD ou d'un DVD multisession

Les disques multisessions permettent d'écrire des données en plusieurs sessions de gravure. Cela s'avère utile, par exemple, pour l'écriture de sauvegardes dont le volume est inférieur à la capacité du support. À chaque session, vous pouvez ajouter un autre fichier de sauvegarde. L'intérêt de cette fonctionnalité est qu'elle n'est pas limitée uniquement aux CD ou DVD de données. Il est également possible d'ajouter des sessions audio sur un disque multisession.

Pour commencer un disque multisession, procédez comme suit :

1. Créez d'abord votre disque de données, puis ajoutez tous les fichiers souhaités. Vous ne pouvez pas commencer par une session CD audio. Veillez à ne pas utiliser toute la capacité du disque ; sinon, vous ne pourrez pas ajouter de nouvelle session.

2. Gravez les données en cliquant sur *Project (Projet)* → *Burn (Graver)*. Une boîte de dialogue apparaît.

3. Accédez à l'onglet *Settings* (Configuration), puis sélectionnez *Start Multisession* (Lancer mode multisession).

4. Si nécessaire, configurez les autres options. Consultez également la Section 9.1, « Création d'un CD de données » (p. 151).

5. Lancez la session de gravure en cliquant sur *Burn* (Graver).

Si le processus de gravure s'est déroulé sans accroc, vous venez de créer un disque multisession. Vous pouvez ajouter autant de sessions que vous le souhaitez, tant que le support dispose d'un espace suffisant. Ne finalisez les disques que lorsque vous êtes certain de ne plus avoir besoin de nouvelles sessions ou que tout l'espace est occupé.

REMARQUE: À propos de l'espace de stockage sur les disques multisessions

Les disques multisessions utilisent une certaine quantité d'espace pour consigner toutes les entrées de vos sessions. L'espace disponible sur le disque est donc moindre et varie en fonction du nombre de sessions utilisées.

9.6 Pour plus d'informations

Outre les deux fonctions principales décrites ci-dessus, K3b offre également d'autres possibilités, comme la création de copies de DVD, la lecture de données audio au format WAV, la regravure de CD ou la lecture de musique au moyen du lecteur audio intégré. Pour obtenir une description détaillée de toutes les fonctionnalités disponibles, consultez le site `http://k3b.sourceforge.net`.



Bureautique

10 Suite bureautique OpenOffice.org

OpenOffice.org est une suite bureautique performante de Linux qui propose des outils pour tous les types de tâches de bureau, tels que l'écriture de textes, l'utilisation de tableurs ou la création de graphiques et de présentations. Grâce à OpenOffice.org, utilisez les mêmes données sur plusieurs plates-formes informatiques. Vous pouvez également ouvrir et modifier les fichiers dans les formats Microsoft Office, puis les enregistrer de nouveau dans ce format, si nécessaire. Ce chapitre présente uniquement les compétences de base nécessaires pour démarrer avec OpenOffice.org. Démarrez l'application à partir du menu SUSE ou avec la commande `ooffice`.

OpenOffice.org comprend plusieurs modules d'application (sous-programmes), conçus pour interagir les uns avec les autres. Il sont répertoriées dans le Tableau 10.1, « Modules d'application OpenOffice.org » (p. 161). Ce chapitre traite plus particulièrement du module Writer. L'aide en ligne comporte une description complète de chaque module, comme l'indique la Section 10.6, « Pour plus d'informations » (p. 169).

Tableau 10.1 *Modules d'application OpenOffice.org*

Writer	Application de traitement de texte performante
Calc	Application de tableur incluant un utilitaire de graphiques
Draw	Application de dessin permettant de créer des dessins vectoriels
Math	Application permettant de générer des formules mathématiques

Impress	Application permettant de créer des présentations
Base	Application de base de données

L'aspect de l'application varie en fonction du bureau et du gestionnaire de fenêtres utilisés. De plus, les formats des boîtes de dialogue d'ouverture et d'enregistrement correspondant à votre bureau sont utilisés. Quelque soit l'aspect du programme, la disposition et les fonctions de base sont identiques.

10.1 Compatibilité avec d'autres applications de bureautique

OpenOffice.org peut travailler avec des documents, des feuilles de calcul, des présentations et des bases de données Microsoft Office. Vous pouvez ouvrir ces documents de façon transparente, comme n'importe quel autre fichier, et les enregistrer dans leur format d'origine. Comme les formats Microsoft sont fermés et que leurs spécifications ne sont pas accessibles aux autres applications, des problèmes de formatage risquent de se produire. Si vous rencontrez des problèmes avec vos documents, ouvrez-les dans l'application d'origine, puis enregistrez-les dans un format ouvert, comme RTF pour les documents texte ou CSV pour les feuilles de calcul.

Pour convertir plusieurs documents, comme lorsque vous utilisez l'application pour la première fois, sélectionnez *File (Fichier)* → *Wizard (Assistant)* → *Document Converter (Conversion de documents)*. Choisissez le format de fichier à partir duquel vous effectuez la conversion. Il existe plusieurs formats StarOffice et Microsoft Office possibles. Après avoir sélectionné un format, cliquez sur *Next (Suivant)*, puis indiquez l'endroit où OpenOffice.org doit rechercher les documents à convertir et où il doit placer les fichiers convertis. Avant de poursuivre, assurez-vous que tous les autres paramètres conviennent. Cliquez sur *Suivant* pour afficher un résumé des actions à exécuter, ce qui offre un autre moyen de contrôler si tous les paramètres sont corrects. Enfin, commencez la conversion en cliquant sur *Convertir*.

IMPORTANT: Recherche de fichiers Windows

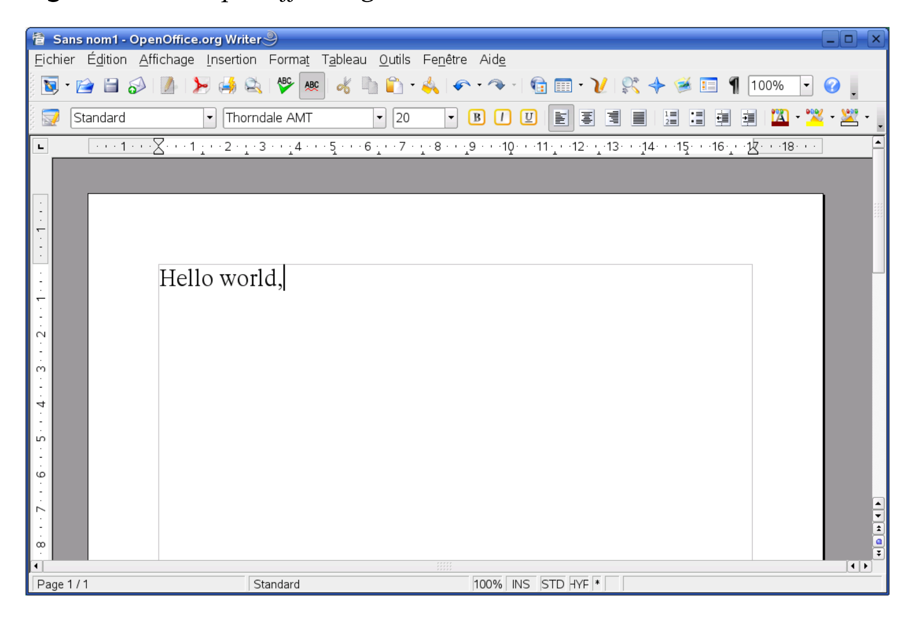
Les documents provenant d'une partition Windows sont généralement placés dans un sous-répertoire du dossier `/windows`.

Pour partager vos documents, vous disposez de plusieurs méthodes. Si le destinataire a uniquement besoin de lire le document, exportez ce dernier au format PDF, avec *File (Fichier) → Export as PDF (Exporter comme PDF)*. Les fichiers PDF peuvent être lus sur n'importe quelle plate-forme, avec une visionneuse comme Adobe Acrobat Reader. Pour partager vos documents en vue d'autoriser leur modification, utilisez l'un des formats standard. Les formats par défaut sont conformes au format XML de la norme OASIS, ce qui les rend compatibles avec un grand nombre d'applications. Les formats TXT et RTF, même si leur formatage est limité, peuvent constituer des solutions satisfaisantes pour les documents contenant du texte. Le CSV est utile pour les feuilles de calcul. OpenOffice.org peut également offrir le format favori de votre destinataire, notamment les formats Microsoft.

OpenOffice.org est disponible pour plusieurs systèmes d'exploitation. Cela en fait un excellent outil pour un groupe d'utilisateurs qui doivent fréquemment partager des fichiers mais dont les ordinateurs ont des systèmes d'exploitation différents.

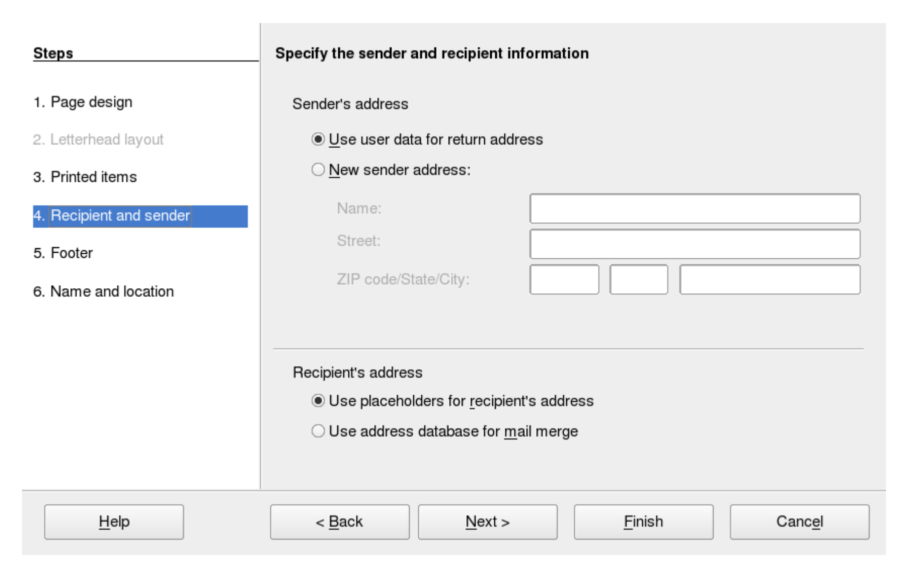
10.2 Traitement de texte avec OpenOffice.org Texte

Figure 10.1 *OpenOffice.org Writer*



Il existe deux manières de créer un document. Pour créer un document de toutes pièces, utilisez *File (Fichier)* → *New (Nouveau)* → *Text Document (Document texte)*. Pour utiliser un format standard et des éléments prédéfinis pour vos propres documents, lancez un assistant. Les assistants sont de petits utilitaires qui vous permettent de prendre des décisions de base, puis créent un document prêt à l'emploi à partir d'un modèle. Par exemple, pour créer une lettre commerciale, sélectionnez *File (Fichier)* → *Wizards (Assistants)* → *Letter (Lettre)*. Les boîtes de dialogue des assistants vous permettent de créer facilement un document de base au format standard. La Figure 10.2, « Assistant OpenOffice.org » (p. 165) présente une boîte de dialogue d'assistant.

Figure 10.2 *Assistant OpenOffice.org*



Entrez le texte dans la fenêtre de document selon vos besoins. Utilisez la barre d'outils *Formatting (Format)* ou le menu *Format* pour modifier l'apparence du document. Utilisez le menu *File (File)* ou les boutons appropriés pour imprimer et enregistrer votre document. À l'aide des options du menu *Insert (Insertion)*, ajoutez des éléments supplémentaires à votre document, comme un tableau, une image ou un graphique.

10.2.1 Sélection de texte

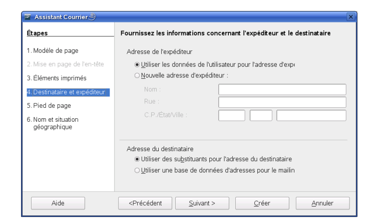
Pour sélectionner du texte, cliquez sur le début de la sélection souhaitée et, tout en maintenant le bouton de la souris enfoncé, déplacez le curseur vers la fin de la zone (il peut s'agir de caractères, de lignes ou de paragraphes entiers). Une fois tout le texte souhaité sélectionné, relâchez le bouton. Une fois sélectionné, le texte apparaît en couleurs inversées. Ouvrez un menu contextuel en cliquant avec le bouton droit de la souris sur la sélection. Utilisez le menu contextuel pour changer la police, le style de la police et d'autres propriétés de texte.

Vous pouvez couper ou copier le texte ainsi sélectionné vers le presse-papiers. Le texte coupé ou copié peut être recollé dans le même document, à un autre endroit. Utilisez le menu contextuel, le menu *Edit (Édition)* ou les icônes de barre d'outils appropriées pour accéder à ces fonctions.

10.2.2 Navigation dans des documents volumineux

Navigator affiche des informations concernant le contenu d'un document. Il permet également de passer rapidement aux autres éléments inclus. Par exemple, utilisez le programme Navigator afin d'obtenir un aperçu rapide de tous les chapitres ou de consulter une liste des images incluses dans le document. Pour l'ouvrir, sélectionnez *Edit (Édition) → Navigator (Navigateur)*. La Figure 10.3, « Navigator dans Writer » (p. 166) montre le navigateur en action. Les éléments listés dans Navigator varient en fonction du document chargé dans Writer.

Figure 10.3 *Navigator dans Writer*



10.2.3 Mise en forme avec des styles

La boîte de dialogue ouverte via *Format → Styles and Formatting (Styles et mise en forme)* vous aide à formater le texte de plusieurs manières. Si vous paramétrez la liste déroulante, en bas de cette boîte de dialogue, sur *Automatic (Automatique)*, OpenOffice.org tente de proposer une sélection de styles adaptés à la tâche. Si vous sélectionnez *All Styles (Tous les styles)*, la liste propose tous les styles du groupe actif. Vous sélectionnez des groupes à l'aide des boutons situés en haut.

Si vous utilisez cette méthode (appelée *formatage souple*) pour formater votre texte, celui-ci n'est pas mis en forme directement. À la place, un style lui est appliqué. Vous pouvez facilement modifier ce style, ce qui entraîne automatiquement un changement de format de tout le texte auquel il est assigné.

Pour assigner un style à un paragraphe, sélectionnez le style à utiliser, puis cliquez sur l'icône représentant un pot de peinture dans *Styles and Formatting (Styles et mise en forme)*. Cliquez sur les paragraphes auxquels vous souhaitez affecter le style. Pour ne

pas assigner de style, appuyez sur Échap ou cliquez à nouveau sur l'icône du pot de peinture.

Vous créez facilement vos propres styles en formatant un paragraphe ou un caractère selon vos souhaits, à l'aide du menu *Format* ou de la barre d'outils de formatage. Sélectionnez l'élément mis en forme dont le style doit être copié. Cliquez ensuite avec le bouton droit de la souris (en maintenant ce bouton enfoncé) à droite du pot de peinture dans *Styles and Formatting (Styles et mise en forme)*, puis sélectionnez *New Style from Selection (Nouveau style à partir de la sélection)* dans le menu qui s'ouvre. Saisissez un nom pour votre style et cliquez sur *OK*. Ce style peut alors être appliqué à d'autres textes.

Vous pouvez facilement changer les détails d'un style en le sélectionnant dans la liste, en cliquant avec le bouton droit de la souris, puis en choisissant *Modify (Modifier)* dans le menu. Ceci permet d'ouvrir une boîte de dialogue dans laquelle toutes les propriétés de formatage possibles peuvent être modifiées.

10.3 Présentation de Calc

Calc est l'application de feuille de calcul d'OpenOffice.org. Vous créez une feuille de calcul via l'option *File (Fichier) → New (Nouveau) → Spreadsheet (Feuille de calcul)* ; pour ouvrir une feuille, utilisez *File (Fichier) → Open (Ouvrir)*. Calc peut lire et enregistrer des documents au format Microsoft Excel.

Dans les cellules de la feuille de calcul, entrez des données fixes ou des formules. Une formule permet de manipuler des données provenant d'autres cellules, afin de générer une valeur dans la cellule où elle est insérée. Vous pouvez également créer des graphiques à partir des valeurs de cellule.

10.4 Présentation d'Impress

Impress est conçu pour créer des présentations destinées à l'affichage sur écran ou à l'impression (sur transparents, par exemple). Vous créez une présentation de toutes pièces avec l'option *File (Fichier) → New (Nouveau) → Presentation (Présentation)*. Pour créer une présentation à l'aide d'un assistant, utilisez *File (Fichier) → Wizards (Assistants) → Presentation (Présentation)*. Ouvrez une présentation existante via *File*

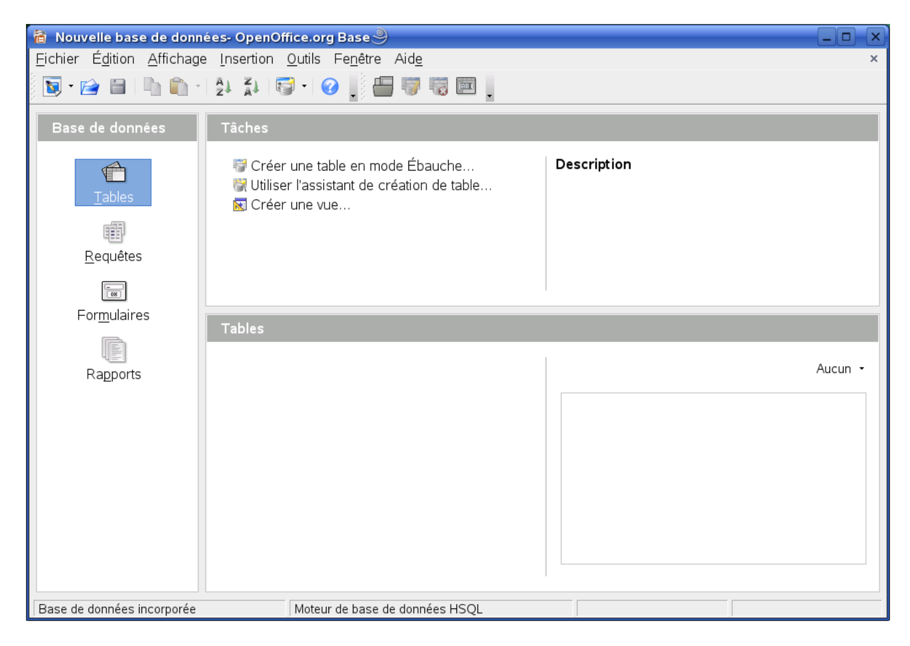
(Fichier) → *Open (Ouvrir)*. Impress peut ouvrir et enregistrer des présentations Microsoft PowerPoint.

10.5 Présentation de Base

OpenOffice 2.0 inclut un nouveau module de base de données. Vous pouvez créer une base de données via l'option *File (Fichier)* → *New (Nouveau)* → *Database (Base de données)*. Un assistant s'ouvre pour vous aider à créer la base de données. Base fonctionne également avec les bases de données Microsoft Access.



Figure 10.4 *Base : bases de données dans OpenOffice.org*



Vous pouvez créer des tables, des formulaires, des requêtes ou des rapports manuellement, ou à l'aide d'assistants très pratiques. Par exemple, l'assistant Table contient un certain nombre de champs courant, destinés à une utilisation professionnelle ou personnelle. Les bases de données créées dans Base peuvent servir de sources de données, comme pour la création de lettres types.

10.6 Pour plus d'informations

OpenOffice.org intègre des options d'informations de divers niveaux. Pour bien connaître un sujet, sélectionnez *Help (Aide) → OpenOffice.org Help (Aide d'OpenOffice.org)*. Le système d'aide contient des informations détaillées concernant chacun des modules d'OpenOffice.org (Writer, Calc, Impress, etc.).

Lors du premier démarrage de l'application, il fournit des *info-bulles* (brèves informations concernant les boutons, affichées lorsque vous placez la souris dessus) et présente les informations de l'*agent d'aide*, qui dépendent des opérations effectuées. Pour obtenir davantage de détails sur les boutons que ceux offerts par les *info-bulles*, utilisez l'option de menu *Help (Aide) → What's This (Qu'est-ce que c'est)*, puis placez la souris sur les boutons voulus. Pour sortir du mode *What's This (Qu'est-ce que c'est)*, cliquez avec la souris. Si vous avez souvent besoin de cette fonction, vous pouvez activer l'option *Extended Tips (Info-bulles étendues)* via *Tools (Outils) → Options → OpenOffice.org → General (Général)*. L'*agent d'aide* et les *info-bulles* peuvent également être activés ou désactivés ici.

Le site Web d'OpenOffice.org est `http://www.openoffice.org`. Il contient des adresses de liste de diffusion, des articles et des informations sur les bogues. Ce site permet également de télécharger les versions de l'application adaptées à divers systèmes d'exploitation.

Evolution : programme de messagerie et de gestion d'agenda 11

Evolution est un logiciel de groupe qui offre les fonctionnalités habituelles de messagerie électronique, ainsi que des fonctionnalités étendues, notamment une liste de tâches et un agenda. Cette application fournit également un carnet d'adresses complet qui permet d'envoyer des informations sur les contacts au format vCard.

Démarrez Evolution à partir du menu principal ou via la commande `evolution`. Lorsque vous démarrez Evolution pour la première fois, vous voyez apparaître un assistant de configuration. Son utilisation est décrite dans la Section 11.3.1, « Configuration de comptes » (p. 174).

IMPORTANT: Comptes Microsoft Exchange

Pour utiliser Evolution avec Microsoft Exchange, vous devez installer le paquetage `ximian-connector`. Installez-le avec YaST.

11.1 Importation des messages électroniques depuis d'autres programmes de messagerie

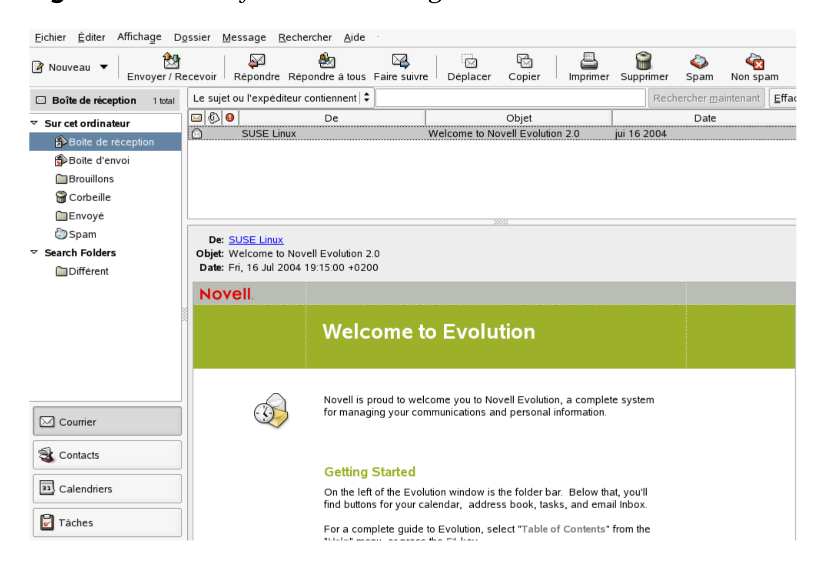
Pour importer des messages électroniques à partir d'autres programmes de messagerie, notamment Netscape, sélectionnez *File (Fichier)* → *Import (Importer)*. Pour les formats mbox, sélectionnez *Import a single file* (Importer un seul fichier). Pour Netscape, sélectionnez *Import data and settings from older programs* (Importer des données et

des paramètres de programmes antérieurs). Pour utiliser des données provenant de programmes utilisant le format maildir, notamment KMail, configurez un compte doté d'un accès au répertoire mail.

11.2 Présentation d'Evolution

La fenêtre par défaut est présentée à la Figure 11.1, « La fenêtre de messagerie d'Evolution » (p. 172). Les menus, éléments de menu et icônes disponibles dans la barre d'outils varient en fonction du composant ouvert. Utilisez le cadre de gauche pour sélectionner les informations à afficher dans le cadre de droite. Ajustez la taille des cadres en faisant glisser les barres de séparation.

***Figure 11.1** La fenêtre de messagerie d'Evolution*



11.2.1 Messagerie

Dans cette vue, la partie supérieure de la fenêtre affiche le contenu du dossier actuel. La partie inférieure est un volet de prévisualisation destiné à afficher le message électronique sélectionné. Pour afficher un autre dossier, sélectionnez-le dans la liste des dossiers située dans le cadre de gauche.

Utilisez la barre de recherche pour rechercher des messages dans un dossier. Pour trier les messages sur la base d'un en-tête de tableau, cliquez sur l'en-tête souhaité. La flèche située à droite indique si la colonne est triée dans l'ordre croissant ou décroissant. Cliquez sur l'en-tête de colonne jusqu'à ce que les messages soient triés dans l'ordre voulu.

11.2.2 Contacts

Cette vue affiche toutes les adresses de votre carnet d'adresses. Pour rechercher une adresse spécifique, utilisez la barre de recherche ou cliquez sur le bouton situé à droite qui affiche la première lettre du nom du contact. Ajoutez des contacts ou des listes avec la barre d'outils.

11.2.3 Calendrier

La première fenêtre affiche la vue du jour. Un volet supplémentaire à droite indique le mois et la liste des tâches. Des vues de la semaine, de la semaine ouvrée et du mois sont également disponibles à partir de la barre d'outils ou du menu *View* (Affichage). Utilisez la barre de recherche pour trouver un rendez-vous saisi dans l'agenda. Ajoutez des rendez-vous et des tâches à l'aide des boutons de la barre d'outils. Vous pouvez également utiliser la barre d'outils pour faire défiler l'agenda page par page ou pour accéder à une date précise.

11.2.4 Tâches

L'option *Tasks* (Tâches) dresse la liste des tâches. Des détails sur la tâche sélectionnée sont fournis dans la partie inférieure de la fenêtre. Utilisez *File (Fichier) → New (Nouveau) → Task (Tâche)* pour ajouter une nouvelle tâche. Effectuez une recherche sur les tâches à l'aide de la barre de recherche. Assignez des tâches à d'autres personnes en cliquant sur le bouton droit de la souris et en sélectionnant *Assign Task* (Assigner une tâche). L'option *Open* (Ouvrir) permet de sélectionner la tâche pour y ajouter des détails, tels que la date de fin et l'état d'avancement.

11.3 Messagerie

Le composant de messagerie Evolution peut fonctionner avec plusieurs comptes dans divers formats. Il offre des fonctionnalités utiles, tels que les dossiers virtuels qui permettent d'afficher les résultats de recherche et de filtrer le courrier indésirable. Configurez l'application via *Edit (Modifier) → Preferences (Préférences)*.

11.3.1 Configuration de comptes

Evolution peut récupérer des messages à partir de plusieurs comptes de messagerie. Lorsque vous composez un message, vous pouvez sélectionner le compte à partir duquel vous souhaitez l'envoyer. Configurez les comptes de messagerie via les options *Edit (Modifier) → Preferences (Préférences) → Mail Accounts (Comptes de messagerie)*. Pour modifier une configuration existante, sélectionnez-la et cliquez sur *Edit (Modifier)*. Pour supprimer un compte, sélectionnez-le et cliquez sur *Delete (Supprimer)*.

Pour ajouter un compte supplémentaire, cliquez sur *Add (Ajouter)*. L'assistant de configuration apparaît. Cliquez sur *Forward* (Suivant) pour l'utiliser. Entrez votre nom et votre adresse de messagerie dans les champs prévus à cet effet. Entrez d'autres informations, si nécessaire. Cochez la case *Make this my default account* (Mon compte par défaut) pour utiliser ce compte par défaut lors de la création de messages. Cliquez sur *Forward* (Suivant).

Sélectionnez le format approprié des messages entrants dans *Server Type* (Type de serveur). *POP* est le format le plus courant de téléchargement de messages à partir d'un serveur distant. *IMAP* fonctionne avec des dossiers de messagerie sur un serveur spécial. Procurez-vous ces informations auprès de votre fournisseur d'accès à Internet ou de l'administrateur du serveur. Remplissez les autres champs nécessaires affichés lorsque le type de serveur est sélectionné. Cliquez sur *Forward* (Suivant) lorsque vous avez terminé. Sélectionnez les *options de réception* souhaitées, si nécessaire. Cliquez sur *Forward* (Suivant).

Configurez ensuite les options de distribution des messages. Pour soumettre un message sortant au système local, sélectionnez *Sendmail*. Pour choisir un serveur distant, sélectionnez *SMTP*. Procurez-vous ces informations auprès de votre fournisseur d'accès à Internet ou de l'administrateur du serveur. Pour le protocole SMTP, remplissez les autres champs qui apparaissent une fois la sélection effectuée. Cliquez sur *Forward* (Suivant) lorsque vous avez terminé.

Par défaut, l'adresse de messagerie est utilisée comme nom pour identifier le compte. Entrez un autre nom si vous le souhaitez. Cliquez sur *Forward* (Suivant). Cliquez sur *Apply* (Appliquer) pour enregistrer la configuration du compte.

Pour faire d'un compte le compte par défaut d'envoi des messages, sélectionnez le compte souhaité, puis cliquez sur *Default* (Par défaut). Pour désactiver la récupération des messages d'un compte, sélectionnez ce dernier et cliquez sur *Disable* (Désactiver). Un compte désactivé peut toujours être utilisé comme adresse d'envoi mais ne permet plus de recevoir de messages entrants. Si nécessaire, réactivez ce compte via l'option *Enable* (Activer).

11.3.2 Création de messages

Pour composer un nouveau message, cliquez sur *New (Nouveau)* → *Mail Message (Message électronique)* . Le fait de répondre à un message ou de le retransmettre ouvre le même éditeur de messages. Dans le champ *From* (De), sélectionnez le compte à partir duquel envoyer le message. Dans les champs cible, entrez une adresse de messagerie ou une partie d'un nom ou d'une adresse de votre carnet d'adresses. Si Evolution trouve une correspondance entre le texte saisi et une entrée du carnet d'adresses, une liste de sélection apparaît. Cliquez sur le contact souhaité ou, si aucune correspondance n'a été détectée, saisissez l'adresse ou le nom intégralement. Pour sélectionner un destinataire directement dans le carnet d'adresses, cliquez sur *To (A)* ou *CC*.

Evolution peut envoyer des messages en texte clair ou au format HTML. Pour formater les messages HTML, sélectionnez *Format* (Format) dans la barre d'outils. Pour envoyer des pièces jointes, sélectionnez *Attach (Joindre)* ou *Insert (Insérer)* → *Attachment (Pièce jointe)* .

Pour envoyer votre message, cliquez sur *Send* (Envoyer). S'il n'est pas prêt à être envoyé immédiatement, effectuez une autre sélection sous *File* (Fichier). Par exemple, enregistrez le message comme brouillon et envoyez-le ultérieurement.

11.3.3 Messages codés et signatures

Evolution prend en charge le codage des messages avec PGP. Il peut signer des messages et contrôler les messages électroniques signés. Pour utiliser ces fonctionnalités, générez et gérez des clés avec une application externe, telle que gpg ou KGpg.

Pour signer un message électronique avant de l'envoyer, sélectionnez *Security (Sécurité) → PGP sign (Signature PGP)*. Lorsque vous cliquez sur *Send (Envoyer)*, une boîte de dialogue vous invite à entrer le mot de passe de votre clé secrète. Saisissez le mot de passe et fermez la boîte de dialogue en cliquant sur *OK* pour envoyer le message signé. Pour signer d'autres messages au cours de la session sans avoir à « déverrouiller » la clé secrète systématiquement, cochez la case *Remember this password for the remainder of this session* (Mémoriser ce mot de passe pour toute la session).

Lorsque vous recevez des messages signés d'autres utilisateurs, un petit cadenas apparaît à la fin du message. Si vous cliquez sur ce symbole, Evolution lance un programme externe (gpg) pour vérifier la signature. Si la signature est valide, une coche verte apparaît à côté du symbole de cadenas. Si elle n'est pas valide, un cadenas cassé apparaît.

Le codage et le décodage des messages sont aussi simples que cela. Après avoir composé le message, sélectionnez *Security (Sécurité) → PGP encrypt (Codage PGP)* et envoyez le message. Lorsque vous recevez des messages codés, une boîte de dialogue vous demande le mot de passe de votre clé secrète. Saisissez le mot de passe pour décoder le message électronique.

11.3.4 Dossiers

Il est souvent pratique de classer les messages électroniques dans différents dossiers. Votre arborescence de dossiers est représentée dans le cadre de gauche. Si vous accédez à votre messagerie par IMAP, les dossiers IMAP sont également représentés dans cette barre de dossiers. Pour POP et la plupart des autres formats, vos dossiers sont stockés localement, triés sous *Local Folders* (Dossiers locaux).

Plusieurs dossiers sont inclus par défaut. *Inbox* (Boîte de réception) est l'endroit où sont placés les nouveaux messages récupérés sur un serveur. L'option *Sent* (Messages envoyés) enregistre des copies des messages électroniques envoyés. *Outbox* (Boîte d'envoi) est le lieu de stockage temporaire des messages qui n'ont pas encore été envoyés. Cette option s'avère utile si vous travaillez hors ligne ou si le serveur de messages sortants est temporairement inaccessible. *Drafts* (Brouillons) permet de stocker les messages électroniques incomplets. Le dossier *Trash* (Corbeille) est destiné au stockage temporaire des éléments supprimés. *Junk* (Courrier indésirable) permet de filtrer le courrier indésirable d'Evolution.

De nouveaux dossiers peuvent être créés sous *On This Computer* (Sur cet ordinateur) ou comme sous-dossiers de dossiers existants. Créez la hiérarchie de dossiers aussi

complexe que vous le souhaitez. Pour créer un dossier, sélectionnez *File (Fichier) → New (Nouveau) → Mail Folder (Dossier de messages)*. Dans la boîte de dialogue des dossiers de messages, entrez le nom du nouveau dossier. Utilisez la souris pour déterminer le dossier parent sous lequel placer le nouveau dossier. Cliquez sur *OK* pour fermer la boîte de dialogue.

Pour déplacer un message dans un dossier, sélectionnez le message en question. Cliquez sur le bouton droit pour ouvrir le menu contextuel. Sélectionnez *Move to Folder* (Déplacer vers le dossier), puis le répertoire de destination dans la boîte de dialogue qui apparaît. Cliquez sur *OK* pour déplacer le message. L'en-tête du message est barré dans le dossier d'origine, ce qui signifie que le message doit être supprimé de ce dossier. Le message est stocké dans le nouveau dossier. Vous pouvez copier des messages en procédant de même.

Le déplacement manuel d'un certain nombre de messages dans des répertoires différents peut nécessiter beaucoup de temps. Vous pouvez utiliser des filtres pour automatiser cette procédure.

11.3.5 Filtres

Evolution offre un certain nombre d'options de filtrage des messages électroniques. Vous pouvez utiliser des filtres pour déplacer un message dans un dossier spécifique ou pour le supprimer. Vous pouvez également déplacer directement des messages dans la corbeille à l'aide d'un filtre. Deux méthodes permettent de créer un filtre : à partir de rien ou à partir du message à filtrer. Cette dernière méthode est extrêmement utile pour filtrer des messages envoyés à une liste de diffusion.

Définition d'un filtre

Sélectionnez *Tools (Outils) → Filters (Filtres)*. La boîte de dialogue qui apparaît répertorie les filtres existants, que vous pouvez modifier ou supprimer. Cliquez sur *Add (Ajouter)* pour créer un filtre. Pour créer un filtre basé sur un message, vous pouvez également sélectionner le message, puis les options *Tools (Outils) → Create Filter from Message (Créer un filtre à partir d'un message)*.

Entrez le nom du nouveau filtre dans *Rule Name* (Nom de la règle). Sélectionnez les critères à utiliser pour le filtre. Les options comprennent notamment l'expéditeur, les destinataires, le compte source, l'objet, la date et l'état. La zone déroulante qui affiche *Contains* (Contient) fournit diverses options, notamment *contains* (contient), *is* (est) et

is not (n'est pas). Sélectionnez la condition appropriée. Entrez le texte à rechercher. Cliquez sur *Add (Ajouter)* pour ajouter d'autres critères de filtrage. Utilisez *Execute actions* (Exécuter les actions) pour déterminer si les critères doivent intégralement ou partiellement être remplis pour que le filtre s'applique.

Dans la partie inférieure de la fenêtre, déterminez l'action à entreprendre lorsque les critères de filtrage sont remplis. Des messages peuvent, par exemple, être déplacés ou copiés vers un dossier ou se voir attribuer une couleur spéciale. En cas de déplacement ou de copie, cliquez sur le dossier de destination pour le sélectionner. Sélectionnez un dossier dans la liste qui apparaît. Pour créer un dossier, cliquez sur *New* (Nouveau). Cliquez sur *OK* lorsque vous avez sélectionné le dossier qui vous convient. Lorsque vous avez terminé la création du filtre, cliquez sur *OK*.

Application de filtres

Les filtres sont appliqués dans l'ordre de leur apparition dans la boîte de dialogue accessible via *Tools (Outils) → Filters (Filtres)*. Modifiez l'ordre en mettant en surbrillance un filtre et en cliquant sur *Up* (Haut) ou *Down* (Bas). Cliquez sur *OK* pour fermer la boîte de dialogue de filtrage lorsque vous avez terminé.

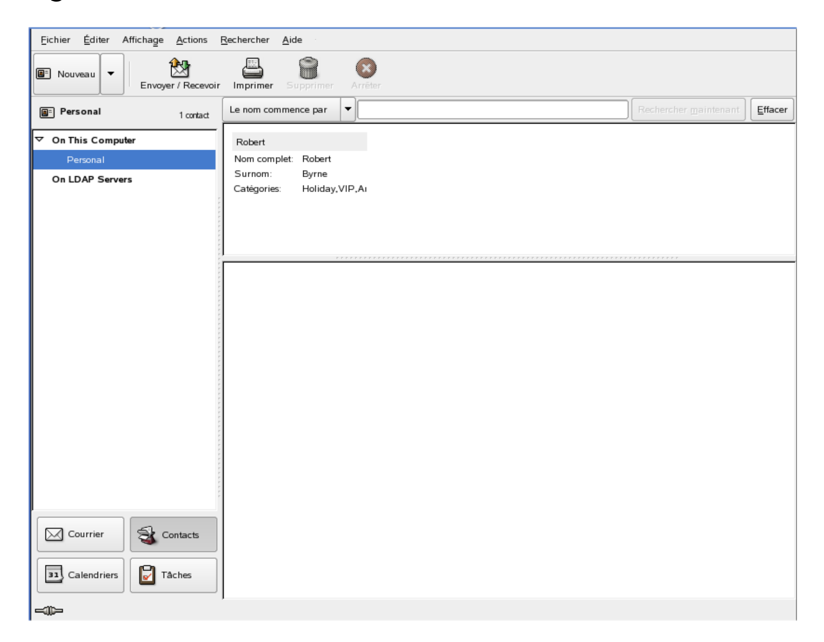
Les filtres s'appliquent à tous les nouveaux messages électroniques. Ils ne sont pas appliqués aux messages déjà présents dans les dossiers. Pour appliquer les filtres aux messages reçus, sélectionnez les messages souhaités, puis cliquez sur *Actions (Actions) → Apply Filters (Appliquer les filtres)*.

11.4 Contacts

Evolution peut utiliser plusieurs carnets d'adresses. Les carnets d'adresses disponibles sont listés dans le cadre de gauche. Recherchez un contact précis à l'aide de la barre de recherche. Ajoutez des contacts dans différents formats au carnet d'adresses Evolution à l'aide de *File (Fichier) → Import (Importer)*. Cliquez avec le bouton droit de la souris sur un contact ; le menu contextuel qui apparaît propose différentes options telles que l'envoi de vos coordonnées ou leur enregistrement au format vCard. Double-cliquez sur un contact pour le modifier.



Figure 11.2 *Le carnet d'adresses Evolution*



11.4.1 Ajout de contacts

Outre le nom et l'adresse électronique, Evolution peut stocker d'autres informations d'adresse et de contact sur une personne. Ajoutez rapidement l'adresse électronique d'un expéditeur en cliquant dessus avec le bouton droit de la souris dans l'aperçu du message. Pour entrer toutes les informations sur un nouveau contact, cliquez sur *New Contact (Nouveau contact)* dans la vue *Contacts* (Contacts). Ces deux méthodes ouvrent une boîte de dialogue dans laquelle vous pouvez entrer des informations sur le contact.

Dans l'onglet *Contact* (Contact), entrez le nom, les adresses électroniques, les numéros de téléphone et les identités de messagerie instantanée du contact. La section *Personal Information* (Informations personnelles) est destinée aux adresses Web et autres informations détaillées. Entrez les autres détails d'adresse du contact dans *Mailing Address* (Adresse de messagerie). Après avoir saisi toutes les informations souhaitées sur le contact, cliquez sur *OK* pour l'ajouter au carnet d'adresses.

11.4.2 Création d'une liste

Si vous envoyez fréquemment des messages électroniques à un ensemble de personnes, simplifiez le processus en créant une liste contenant toutes les adresses concernées. Cliquez sur *File (Fichier) → New (Nouveau) → Contact List (Liste de contacts)*. L'éditeur de liste de contacts apparaît. Entrez le nom de la liste. Ajoutez les adresses en les tapant dans la zone prévue à cet effet, puis en cliquant sur *Add (Ajouter)* ou en faisant glisser des contacts de la vue *Contacts* (Contacts) jusqu'à cette zone. Activez et désactivez *Hide addresses* (Masquer les adresses) pour déterminer si les destinataires peuvent voir les autres destinataires du message. Cliquez sur *OK* lorsque vous avez terminé. La liste fait désormais partie de vos contacts et apparaît dans la fenêtre de composition dès que vous en saisissez les premières lettres.

11.4.3 Ajout de carnets d'adresses

Configurez d'autres carnets d'adresses GroupWise et Exchange dans la configuration de ce compte. Pour ajouter d'autres carnets d'adresses locaux ou LDAP, sélectionnez *File (Fichier) → New (Nouveau) → Address Book (Carnet d'adresses)*. Dans la boîte de dialogue qui apparaît, sélectionnez le type du carnet d'adresses et entrez les informations requises.

11.5 Agendas

Evolution peut fonctionner avec plusieurs agendas. Sélectionnez *File (Fichier) → Import (Importer)*, pour importer des agendas au format iCalendar. La fonction d'agenda permet de noter des rendez-vous et de planifier des réunions. Si vous le souhaitez, définissez des rappels destinés à vous informer à quel moment doivent commencer vos rendez-vous planifiés.

Figure 11.3 L'agenda Evolution

11.5.1 Ajout de rendez-vous

Pour ajouter un nouveau rendez-vous à votre agenda, cliquez sur *File (Fichier)* → *New (Nouveau)* → *Appointment (Rendez-vous)*. Dans l'onglet *Appointment* (Rendez-vous), entrez les informations concernant le rendez-vous. Sélectionnez une catégorie, si nécessaire, pour simplifier la recherche et le tri ultérieurs. Utilisez éventuellement l'option *Alarm* (Alarme) pour définir une alarme afin qu'Evolution vous rappelle vos rendez-vous. Si le rendez-vous a lieu régulièrement, définissez des dates récurrentes via *Recurrence* (Récurrence). Cliquez sur *OK* après avoir effectué tous les paramétrages. Le nouveau rendez-vous apparaît alors dans votre agenda.

11.5.2 Planification d'une réunion

Pour planifier une réunion avec d'autres personnes, sélectionnez *File (Fichier)* → *New (Nouveau)* → *Meeting (Réunion)*. Entrez les informations comme s'il s'agissait d'un rendez-vous. Ajoutez les participants dans *Invitations* (Invitations) ou *Scheduling* (Planification). Pour entrer des participants à partir du carnet d'adresses, utilisez *Contacts* (Contacts) pour ouvrir la liste des contacts de votre carnet d'adresses. L'option de *planification* sert également à planifier l'heure qui convient à tous les participants. Après

avoir configuré les participants, cliquez sur *Autopick* (Sélection automatique) pour rechercher automatiquement l'heure appropriée.

11.5.3 Ajout d'agendas

Les agendas GroupWise et Exchange doivent être configurés dans la configuration du compte. Pour ajouter des agendas locaux ou Web supplémentaires, sélectionnez *File (Fichier)* → *New (Nouveau)* → *Calendar (Agenda)*. Sélectionnez le type souhaité et entrez les informations requises.

11.6 Synchronisation des données avec un périphérique de poche

Vous pouvez synchroniser les données d'Evolution avec des périphériques de poche, tels qu'un Palm. La synchronisation utilise le pilote GNOME. Sélectionnez *Tools (Outils)* → *Pilot Settings (Paramètres du pilote)* pour ouvrir l'assistant de configuration. Consultez l'aide pour plus d'informations.

11.7 Evolution pour les utilisateurs GroupWise

Les utilisateurs de GroupWise devraient facilement pouvoir accéder à leurs comptes GroupWise avec Evolution. Evolution et GroupWise utilisent une terminologie très semblable. Les personnes qui utilisent déjà un système doivent pouvoir facilement se familiariser avec un autre système.

11.7.1 Configuration d'Evolution pour accéder à votre système GroupWise

Utilisez l'assistant de configuration de messagerie Evolution pour configurer Evolution de sorte qu'il accède au système GroupWise. Pour lancer l'assistant de configuration

de messagerie Evolution, cliquez sur *Preferences (Préférences)* → *Mail Accounts (Comptes de messagerie)* → *Add (Ajouter)*, puis sur *Forward* (Suivant).

Sur la page Identity (Identité), indiquez votre adresse électronique dans le système GroupWise (par exemple, jean@exemple.com), puis cliquez sur *Forward* (Suivant).

Sur la page des messages entrants, sélectionnez *IMAP* dans la liste des types de serveurs et indiquez le nom d'hôte de votre serveur GroupWise dans le champ prévu à cet effet. Au besoin, définissez sur cette page les autres paramètres nécessaires à votre système, puis cliquez sur *Forward* (Suivant).

Sur la page des messages sortants, sélectionnez *SMTP* dans la liste des types de serveurs et indiquez le nom d'hôte de votre serveur GroupWise dans le champ prévu à cet effet. Au besoin, définissez sur cette page les autres paramètres nécessaires à votre système, puis cliquez sur *Forward* (Suivant).

Dans la page de gestion des comptes Account Management, indiquez le nom que vous souhaitez utiliser pour identifier ce compte sur la page Evolution Settings (Paramètres Evolution), puis cliquez sur *Forward* (Suivant).

Cliquez sur *Apply* (Appliquer) pour créer le compte GroupWise. Votre boîte aux lettres GroupWise apparaît alors dans la liste des comptes de messagerie disponibles.

11.8 Pour plus d'informations

Evolution propose des pages d'aide très complètes. Utilisez le menu *Help* (Aide) pour accéder à ces informations. Pour plus d'informations sur Evolution, consultez le site Web de ce projet à l'adresse `http://www.gnome.org/projects/evolution/`
.

Kontact : programme de messagerie et de gestion d'agenda 12

Kontact réunit les fonctionnalités de plusieurs applications KDE au sein d'une même interface conviviale, destinée à la gestion des informations personnelles. Ces applications sont : KMail pour la messagerie, KOrganizer pour l'agenda, KAddressbook pour les contacts et KNotes pour les notes. Il est également possible de synchroniser les données à l'aide de périphériques externes, tels qu'un PalmPilot ou tout autre périphérique de poche. Kontact s'intègre facilement au reste du bureau KDE et se connecte à un large éventail de serveurs Groupware. Il offre des fonctionnalités supplémentaires, telles que le filtrage des virus et des courriers indésirables, ainsi qu'un lecteur RSS.

Pour démarrer Kontact, cliquez sur *Office (Bureautique) → Kontact - Personal Information Manager (Kontact - Gestionnaire d'informations personnelles)* dans le menu principal. Vous pouvez également entrer `kontact` dans une ligne de commande. Si vous n'avez besoin que d'une fonctionnalité donnée, vous pouvez ouvrir uniquement le composant correspondant au lieu de l'application complète.

12.1 Importation des messages électroniques depuis d'autres programmes de messagerie

Pour importer des messages électroniques d'autres applications, sélectionnez *Tools (Outils) → Import Messages (Importer des messages)* dans la vue de messagerie de Kontact. Il comprend notamment des filtres d'importation pour Outlook Express, le format mbox, le format de messagerie texte, Pegasus Mail, Opera et Evolution. Vous

pouvez également démarrer l'utilitaire d'importation séparément, à l'aide de la commande `kmailcvt`.

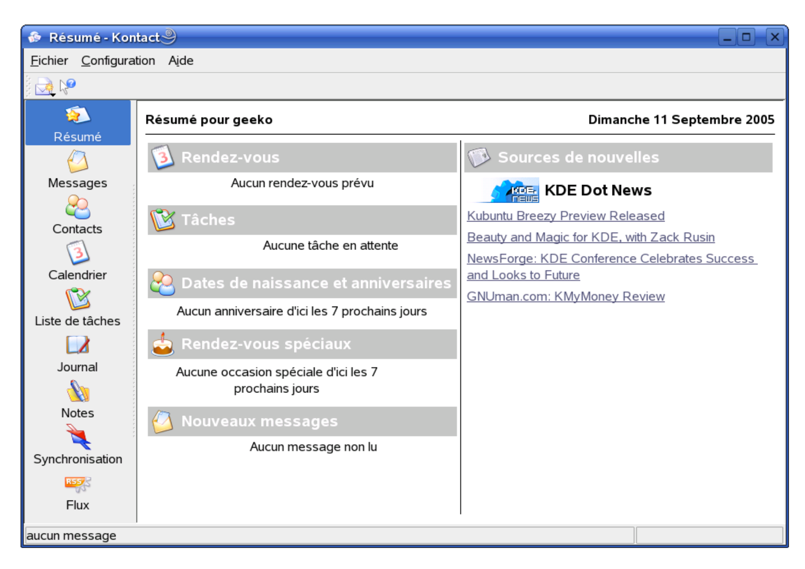
Sélectionnez l'application correspondante, puis confirmez votre choix en cliquant sur *Continue* (Continuer). Un fichier ou un dossier vous est demandé en fonction du type sélectionné. Kontact finalise ensuite le processus.

12.2 Présentation de Kontact

La fenêtre par défaut affiche la page *Summary* (Résumé) (consultez la Figure 12.1, « Vue Summary (Résumé) de la fenêtre Kontact » (p. 186)). Utilisez les boutons de gauche pour accéder aux composants correspondants.

La fonction *Summary* (Résumé) fournit des informations de base : anniversaires à souhaiter, liste des tâches à effectuer, informations météo, statut de KPilot, etc. Grâce aux sources RSS auxquelles elle peut accéder, la section News (Informations) vous fournit des informations intéressantes, tenues à jour. Sélectionnez *Settings (Configuration)* → *Configure Summary View (Configurer la vue résumée)* pour configurer le mode d'affichage des informations.

***Figure 12.1** Vue Summary (Résumé) de la fenêtre Kontact*



12.2.1 Messagerie

Située à gauche de l'écran, la zone des dossiers contient une liste de vos dossiers de messages (boîtes aux lettres) avec, à chaque fois, le nombre total de messages et le nombre de messages non lus. Pour sélectionner un dossier, cliquez simplement dessus. Les messages qu'il contient apparaissent dans le cadre supérieur droit. Le nombre de messages dans ce dossier apparaît également dans la barre d'état au bas de la fenêtre d'application.

Le sujet, l'expéditeur et l'heure de réception de chacun des messages reçus sont indiqués dans la zone d'en-tête à droite. Cliquez un message pour le sélectionner et l'afficher dans la fenêtre du message. Triez les messages en cliquant sur une des colonnes (sujet, expéditeur, date, etc.). Le contenu du message sélectionné apparaît dans le cadre de la fenêtre réservé à cet effet. Les pièces jointes sont représentées par des icônes à la fin du message, en fonction de leur type MIME, ou peuvent être affichées en mode « in-line ».

Les messages peuvent être marqués au moyen de différents drapeaux d'état. Pour modifier l'état, allez dans *Message → Mark Message (Marquer comme message)*. Cette fonctionnalité vous permet d'affecter un état à un message (Important ou Ignoré, par exemple). Vous pouvez, par exemple, mettre en surbrillance les messages importants à ne pas oublier. Pour n'afficher que les messages présentant un état particulier, utilisez la fonction *Status* (États) dans la barre de recherche.

12.2.2 Contacts

Le cadre supérieur gauche de ce composant affiche toutes les adresses contenues dans les carnets d'adresses actuellement activés. Le cadre inférieur gauche répertorie vos carnets d'adresses et indique s'ils sont actuellement actifs. Le cadre de droite affiche le contact sélectionné. Utilisez la barre de recherche située en haut de l'écran pour rechercher un contact en particulier.

12.2.3 Liste des tâches

L'option *To-do List* (Liste des tâches) répertorie les tâches à effectuer. Cliquez sur le champ situé en haut de la page pour ajouter une nouvelle entrée à la liste. Cliquez avec le bouton droit de la souris sur la colonne d'une entrée existante pour modifier la valeur

de cette colonne. Il est possible de décomposer une entrée en plusieurs sous-entrées. Cliquez sur une entrée avec le bouton droit de la souris, puis sur *New Sub-to-do* (Nouvelle sous-tâche) pour créer une sous-entrée. Vous pouvez également affecter des tâches à d'autres personnes.

12.2.4 Calendrier

La vue de l'agenda comporte différents cadres. Elle affiche, par défaut, un petit agenda du mois en cours et une vue de la semaine en cours. Elle inclut également la liste des tâches à effectuer, une vue détaillée de l'événement ou de la tâche en cours, ainsi qu'une liste des agendas accompagnés de leur état respectif. Sélectionnez une vue différente dans la barre d'outils ou dans le menu *View* (Affichage).

12.2.5 Notes

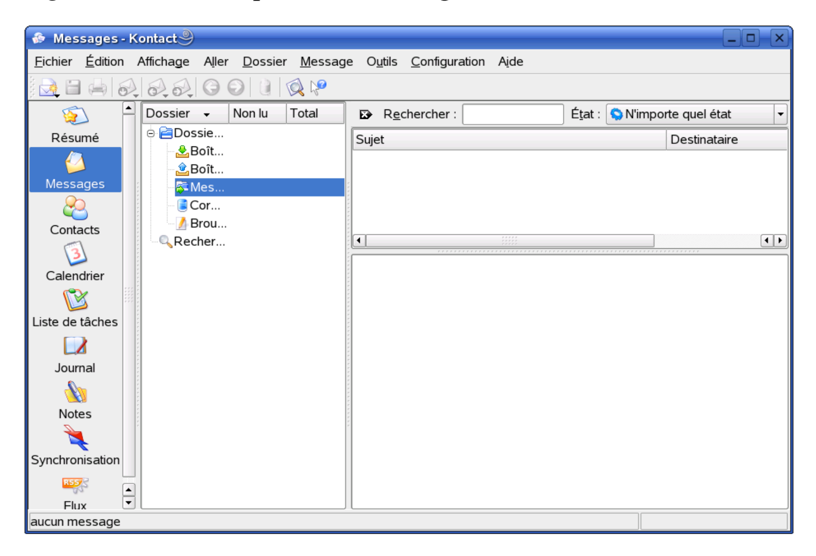
Utilisez le composant Notes comme pense-bête. Si vous utilisez KDE, cliquez sur l'icône KNote dans la barre système pour que vos notes soient visibles sur le bureau.

12.3 Messagerie

Kontact utilise KMail comme composant de messagerie. Pour configurer ce composant de messagerie, ouvrez-le, puis sélectionnez *Settings (Configuration) → Configure KMail (Configurer KMail)*. Client de messagerie complet, KMail prend en charge un grand nombre de protocoles. Le menu *Tools* (Outils) contient plusieurs fonctions utiles pour la gestion du courrier indésirable. Utilisez le champ *Find* (Recherche) pour effectuer une recherche détaillée des messages. Grâce à l'option *Anti-Spam Wizard* (Assistant de gestion des messages non sollicités), vous gérez des outils capables de filtrer le courrier publicitaire indésirable. L'*Anti-Virus Wizard* (Assistant de gestion des virus), quant à lui, permet de gérer les systèmes d'analyse des virus transmis par courrier électronique. Ces deux assistants fonctionnent avec un logiciel externe de gestion des virus et du courrier indésirable. Si ces options sont désactivées, installez des solutions complémentaires afin d'assurer une protection contre les virus et le courrier indésirable.



***Figure 12.2** Composant de messagerie de Kontact*



12.3.1 Configuration de comptes

Kontact peut gérer plusieurs comptes de messagerie : votre adresse électronique privée et votre adresse professionnelle, par exemple. Lorsque vous rédigez un message électronique, sélectionnez l'une des identités définies précédemment ; pour ce faire, cliquez sur *View (Affichage)* → *Identity (Identité)*. Pour créer un profil d'identité, sélectionnez *Settings (Configuration)* → *Configure KMail (Configurer KMail)*, puis *Identities (Identités)* → *New (Nouveau)*. Dans la boîte de dialogue qui apparaît, attribuez un nom à la nouvelle identité, tel que « privée » ou « professionnelle ». Cliquez sur *OK* pour ouvrir une boîte de dialogue dans laquelle vous pourrez entrer des informations supplémentaires. Vous pouvez également assigner une identité à un dossier de sorte que, lorsque vous répondez à un message contenu dans ce dossier, l'identité assignée soit sélectionnée.

Sous *General* (Général), tapez votre nom, le nom de votre organisation et votre adresse électronique. Sous *Cryptography* (Cryptographie), sélectionnez les clés permettant d'envoyer des messages codés ou dotés d'une signature numérique. Pour que le codage fonctionne, commencez par créer une clé à l'aide de KGpg (consultez le Chapitre 6, *Le chiffrement avec KGpg* (p. 107)).

Sous *Advanced* (Options avancées), vous pouvez indiquer une adresse de réponse et une adresse de copie carbone cachée, choisir un dictionnaire, sélectionner les dossiers dans lesquels placer les brouillons et les messages envoyés, et définir le mode d'envoi des messages. Sous *Signature*, indiquez si chacun de vos messages doit comporter une signature (et si oui, quel type), sous la forme d'un bloc de texte supplémentaire ajouté à la fin du message. Vous pouvez, par exemple, inclure vos coordonnées à la fin de chaque message électronique. Pour activer cette option, sélectionnez *Enable Signature* (Activer la signature), puis indiquez si la signature provient d'un fichier, d'un champ de saisie ou de l'exécution d'une commande. Une fois les paramètres d'identité définis, confirmez votre choix en cliquant sur *OK*.

Les paramètres qui apparaissent sous *Network* (Réseau) déterminent le mode de réception et d'envoi des messages électroniques par Kontact. L'écran se compose de deux onglets : un pour l'envoi, l'autre pour la réception du courrier. Ces paramètres varient, pour leur plus grand nombre, en fonction du système et du réseau dans lequel se situe votre serveur de messagerie. Si vous n'êtes pas certain des paramètres ou des éléments à sélectionner, consultez votre fournisseur de services Internet ou votre administrateur système.

Pour créer des boîtes destinées aux messages sortants, dans l'onglet *Sending* (Envoi), cliquez sur *Add* (Ajouter). Choisissez le type de transport SMTP ou sendmail. SMTP apparaît comme le choix le plus judicieux dans la plupart des cas. Une fois ce choix enregistré, une fenêtre apparaît pour vous permettre de communiquer les données relatives à votre serveur SMTP. Indiquez un nom et entrez l'adresse du serveur (telle que vous l'a communiquée votre fournisseur de services Internet). Si le serveur vous demande de vous authentifier, activez l'option *Server requires authentication* (Le serveur exige une identification). Les paramètres de sécurité sont regroupés dans *l'onglet* Sécurité. Spécifiez votre méthode de chiffrement préférée.

L'onglet *Réception* regroupe les paramètres de réception du courrier électronique. Utilisez *Ajouter* pour créer un compte. Choisissez une des différentes méthodes de récupération du courrier, à savoir local (stocké au format Mbox ou MailDir), POP3 ou IMAP. Définissez des paramètres adaptés à votre serveur.

12.3.2 Création de messages

Pour rédiger de nouveaux messages, sélectionnez *Message → New Message (Nouveau message)* ou cliquez sur l'icône correspondante dans la barre d'outils. Pour envoyer des messages à partir de comptes de messagerie différents, sélectionnez une des identités

selon la procédure détaillée dans la Section 12.3.1, « Configuration de comptes » (p. 189). Dans le champ *To* (À), entrez une adresse électronique, ou une partie d'un nom ou d'une adresse figurant dans votre carnet d'adresses. Si Kontact trouve une correspondance entre le texte saisi et une entrée du carnet d'adresses, une liste de sélection apparaît. Cliquez sur le contact souhaité ou, si aucune correspondance n'a été détectée, saisissez l'adresse ou le nom intégralement. Pour sélectionner directement une entrée du carnet d'adresses, cliquez sur le bouton ... situé en regard du champ d'adresse.

Pour joindre un fichier à votre message, cliquez sur l'icône de trombone et sélectionnez le fichier. Vous pouvez aussi glisser un fichier depuis le bureau ou un autre dossier et le déposer dans la fenêtre *Nouveau message*, ou sélectionner une des options du menu *Joindre*. Le format d'un fichier est généralement correctement identifié. Si tel n'est pas le cas, cliquez sur l'icône correspondante à l'aide du bouton droit de la souris. Un menu apparaît ; sélectionnez *Properties* (Propriétés). Définissez le format et le nom de fichier dans la boîte de dialogue suivante, et ajoutez une description. En outre, indiquez si le fichier joint doit être signé ou codé.

Une fois votre message composé, envoyez-le immédiatement en cliquant sur *Message → Send (Envoyer)*, ou placez-le dans la boîte d'envoi en sélectionnant *Message → Queue (Mettre dans la file d'attente)*. Si vous envoyez le message électronique et que l'envoi aboutit, le message est copié dans le dossier des messages envoyés, `sent-mail`. Vous pouvez modifier ou supprimer tout message placé dans la `boîte d'envoi`.

12.3.3 Messages codés et signatures

Pour ce faire, vous devez d'abord générer une paire de clés (consultez le Chapitre 6, *Le chiffrement avec KGpg* (p. 107)). Vous pouvez configurer les détails de la procédure de codage : sélectionnez *Settings (Configuration) → Configure KMail (Configurer KMail) → Identities (Identités)* pour indiquer l'identité sous laquelle envoyer les messages signés et codés. Cliquez ensuite sur *Modify* (Modifier). Cliquez sur *OK* pour confirmer votre choix ; la clé doit apparaître dans le champ correspondant. Cliquez sur *OK* pour fermer la boîte de dialogue de configuration.

12.3.4 Dossiers

Les dossiers de la messagerie vous permettent de classer vos messages. Par défaut, les messages sont stockés dans le répertoire `~/.kde/share/apps/kmail/mail`. Lors du premier démarrage de KMail, le programme crée plusieurs dossiers. Les

nouveaux messages extraits d'un serveur sont initialement placés dans le dossier `inbox` (boîte de réception). Le dossier `outbox` (boîte d'envoi) constitue une zone de stockage temporaire des messages en attente d'expédition. Le dossier `sent-mail` (messages envoyés) contient les copies des messages envoyés. Le dossier `trash` (corbeille) comprend une copie de tous les messages électroniques supprimés à l'aide de la touche Suppr ou de l'option *Edit (Modifier) → Delete (Supprimer)*. Enfin, le dossier `drafts` (brouillons) permet de stocker tous les messages incomplets. Si vous utilisez le protocole de messagerie IMAP, les dossiers IMAP apparaissent en dessous des dossiers locaux. Les dossiers de chaque serveur de courrier entrant (serveur local ou IMAP, par exemple) apparaissent dans la liste des dossiers.

Si vous avez besoin de dossiers supplémentaires pour classer vos messages, créez-en en sélectionnant *Folder (Dossier) → New Folder (Nouveau dossier)*. Une fenêtre apparaît, dans laquelle vous devez indiquer le nom et le format du nouveau dossier.

Cliquez avec le bouton droit de la souris sur le dossier ; le menu contextuel qui apparaît propose différentes opérations pouvant être effectuées sur les dossiers. Cliquez sur *Expire* (Délai d'expiration) pour indiquer la date d'expiration des messages lus et non lus, l'action à entreprendre après expiration, et si les messages ayant expiré doivent être supprimés ou placés dans un dossier donné. Si vous souhaitez utiliser le dossier pour stocker les messages d'une liste de diffusion, définissez les options nécessaires dans *Folder (Dossier) → Mailing List Management (Gestion des listes de diffusion)*.

Pour déplacer des messages d'un dossier à l'autre, sélectionnez-les, puis appuyez sur M ou cliquez sur *Message → Déplacer vers*. Une liste de dossiers apparaît. Sélectionnez le dossier dans lequel vous voulez déplacer votre message. Une autre manière de déplacer des messages consiste à les faire glisser de la fenêtre supérieure vers le dossier de votre choix dans la fenêtre de gauche.

12.3.5 Filtres

Les filtres constituent une méthode pratique de traitement automatique des messages entrants. Ils utilisent différents éléments des messages, tels que leur taille ou leur expéditeur, afin de déterminer l'action à entreprendre : placer les messages dans des dossiers particuliers, supprimer les messages indésirables ou renvoyer des messages à l'expéditeur, par exemple.

Définition d'un filtre

Pour créer entièrement un filtre, sélectionnez *Settings (Configuration) → Configure Filters (Configurer les filtres)*. Pour créer un filtre sur la base d'un message existant, sélectionnez le message souhaité dans la liste des en-têtes, cliquez sur *Tools (Outils) → Create Filter (Créer un filtre)*, puis choisissez les critères de filtre souhaités.

Sélectionnez la méthode de mise en correspondance des critères de filtre (l'un d'eux ou tous). Sélectionnez ensuite les critères à appliquer uniquement aux messages souhaités. Dans la zone *Filter Actions* (Actions du filtre), définissez l'opération que le filtre doit effectuer sur les messages répondant aux critères indiqués. L'option *Advanced Options* (Options avancées) permet de définir le moment auquel le filtre est appliqué et si des filtres supplémentaires doivent être pris en compte pour ces messages.

Application de filtres

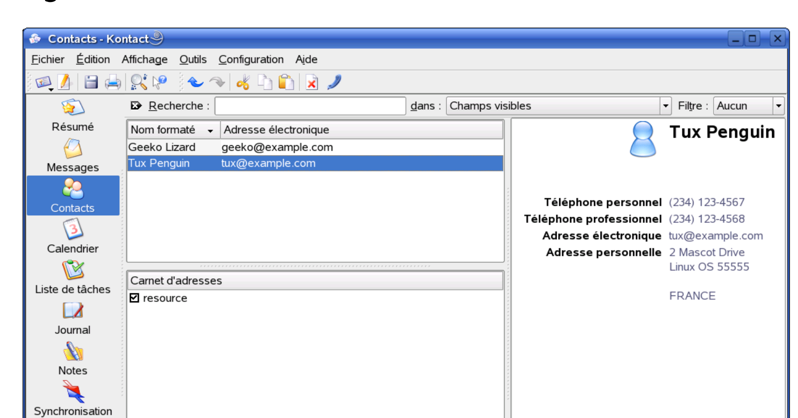
Les filtres sont appliqués dans l'ordre de leur apparition dans la boîte de dialogue accessible via *Settings (Configuration) → Configure Filters (Configurer les filtres)*. Pour modifier cet ordre, sélectionnez un filtre et cliquez sur les boutons fléchés. Les filtres sont uniquement appliqués aux nouveaux messages reçus ou envoyés, conformément aux options avancées du filtre. Pour appliquer les filtres aux messages existants, sélectionnez les messages souhaités, puis cliquez sur *Message → Apply Filters (Appliquer les filtres)*.

Si les filtres définis ne donnent pas le résultat escompté, contrôlez-les en cliquant sur *Tools (Outils) → Filter Log Viewer (Afficheur des journaux de filtrage)*. Lorsque la fonction de consignation est activée dans cette boîte de dialogue, elle indique la manière dont les filtres traitent les messages, ce qui peut vous aider à identifier le problème.

12.4 Contacts

Le composant propre aux contacts utilise KAddressBook. Pour le configurer, cliquez sur *Settings (Configuration) → Configure KAddressBook (Configurer KAddressBook)*. Pour rechercher un contact précis, utilisez la barre de recherche. Avec l'option *Filter* (Filtrer), vous pouvez n'afficher que les contacts d'une catégorie donnée. Cliquez avec le bouton droit de la souris sur un contact ; le menu contextuel qui apparaît propose différentes options telles que l'envoi de vos coordonnées dans un message électronique.

Figure 12.3 *Le carnet d'adresses Kontact*



12.4.1 Ajout de contacts

Pour ajouter un contact en utilisant les nom et adresse électronique d'un message, cliquez avec le bouton droit de la souris sur le composant de message, puis sélectionnez *Open in Address Book* (Ouvrir dans le carnet d'adresses). Pour ajouter un nouveau contact sans utiliser les informations d'un message électronique, sélectionnez *File (Fichier)* → *New Contact (Nouveau contact)* dans le composant d'adresse. Ces méthodes ouvrent toutes deux une boîte de dialogue dans laquelle vous pouvez entrer des informations sur le contact.

Dans l'onglet *General* (Général), entrez les principales informations de contact (nom, adresses électroniques, numéros de téléphone, etc.). Les catégories permettent de trier les adresses. La zone *Details* (Détails) contient des informations plus spécifiques, telles que la date d'anniversaire et le nom du conjoint.

Si votre contact utilise une messagerie instantanée, vous pouvez ajouter ces identités dans *IM Addresses* (Adresses IM). Si vous effectuez cette opération, et que Kopete ou un autre programme de discussion (chat) KDE fonctionne en même temps que Kontact, vous pouvez afficher les informations sur l'état de ces identités dans Kontact. Dans *Crypto Settings* (Configuration du codage), entrez les données de codage du contact, telles que la clé publique.

La zone *Misc* (Divers) comporte des informations supplémentaires, notamment une photo et l'emplacement des informations de disponibilité (disponible/occupé) de l'utilisateur. Utilisez *Custom Fields* (Champs personnalisés) pour ajouter vos propres informations au contact ou au carnet d'adresses.

Vous pouvez également importer les contacts dans différents formats. Sélectionnez *File (Fichier) → Import (Importer)*, puis le format souhaité. Sélectionnez ensuite le fichier à importer.

12.4.2 Création d'une liste de distribution

Si vous envoyez souvent des messages électroniques au même groupe de personnes, vous pouvez créer une liste de distribution ; ce système vous permet de réunir plusieurs adresses électroniques dans un même élément de contact, ce qui vous évite d'entrer le nom de chaque destinataire dans chaque message que vous envoyez à ce groupe. Cliquez d'abord sur *Settings (Configuration) → Show Extension Bar (Afficher la barre d'extension) → Distribution List Editor (Éditeur de listes de distribution)*. Dans la nouvelle section qui apparaît, cliquez sur *New List* (Nouvelle liste). Saisissez un nom pour votre style et cliquez sur *OK*. Pour ajouter des contacts à la liste, faites-les glisser depuis la liste des adresses et placez-les dans la fenêtre de liste de distribution. Utilisez cette liste de la même manière qu'un simple contact lorsque vous créez un message.

12.4.3 Ajout de carnets d'adresses

IMPORTANT: Carnets d'adresses Groupware

Le meilleur moyen d'ajouter des ressources Groupware consiste à utiliser un outil distinct, l'assistant Groupware. Pour ce faire, fermez Kontact, puis exécutez la commande `groupwarewizard` sur une ligne de commande ou à partir de la suite bureautique du menu KDE. Sélectionnez le type de serveur, tel que SLOX, GroupWise ou Exchange, dans la liste proposée, puis entrez l'adresse et les données d'authentification. L'assistant ajoute alors à Kontact les ressources disponibles.

Kontact peut accéder à plusieurs carnets d'adresses, tels que les carnets partagés Novell GroupWise ou un serveur LDAP. Sélectionnez *Settings (Configuration) → Show Extension Bar (Afficher la barre d'extension) → Address Books (Carnets d'adresses)* pour

afficher les carnets d'adresses actuels. Cliquez sur *Add* (Ajouter) pour ajouter un carnet, puis sélectionnez son type et indiquez enfin les informations requises.

Les cases à cocher situées en regard des carnets d'adresses indiquent l'état d'activation de chaque carnet. Pour masquer un carnet sans le supprimer, désélectionnez la case correspondante. Cliquez sur *Remove* (Supprimer) pour supprimer de la liste le carnet sélectionné.

12.5 Calendrier

Kontact utilise KOrganizer comme composant d'agenda. Pour le configurer, sélectionnez *Settings (Configuration) → Configure KOrganizer (Configurer KOrganizer)*. La fonction d'agenda permet de noter des rendez-vous et de planifier des réunions. Si vous le souhaitez, le système peut vous envoyer un rappel des événements à venir. Vous pouvez également importer, exporter et archiver les agendas à l'aide des options du menu *File* (Fichier).

Figure 12.4 *Agenda de Kontact*

12.5.1 Planification d'un événement

Pour ajouter un événement ou une réunion, cliquez sur *Actions → New Event (Nouvel événement)*. Entrez les détails souhaités. Sous *Reminder* (Rappel), indiquez le moment

exact (nombre de minutes, d'heures ou de jours à l'avance) où l'événement doit être rappelé aux participants. Dans le cas d'un événement récurrent, indiquez l'intervalle correspondant. Une autre méthode de création d'un événement en un point donné de l'agenda consiste à double-cliquer sur le champ correspondant dans l'une des vues d'agenda du programme. Une boîte de dialogue apparaît, identique à celle obtenue via le menu. Vous pouvez également sélectionner une plage horaire dans la vue Agenda, puis cliquer dessus avec le bouton droit de la souris.

Pour indiquer les personnes participant à un événement, entrez leurs données manuellement dans la boîte de dialogue ou insérez ces données depuis le carnet d'adresses. Pour entrer des données manuellement, sélectionnez *New* (Nouveau). Pour importer des données depuis le carnet d'adresses, cliquez sur *Select Addressee* (Sélectionner le destinataire), puis sélectionnez les entrées correspondantes dans la boîte de dialogue. Pour planifier l'événement en fonction des disponibilités des participants, cliquez sur *Pick Date* (Choisir la date) dans *Free/Busy* (Disponibilités).

Utilisez l'onglet *Recurrence* (Périodicité) pour configurer un événement qui se produit de manière régulière. La fonction *Attachments* (Pièces jointes) s'avère pratique pour lier d'autres informations à l'événement, par exemple, l'ordre du jour d'une réunion.

12.5.2 Ajout d'agendas

IMPORTANT: Agendas Groupware

Le meilleur moyen d'ajouter des ressources Groupware consiste à utiliser un outil distinct, l'assistant Groupware. Pour ce faire, fermez Kontact, puis exécutez la commande `groupwarewizard` sur une ligne de commande ou à partir de la suite bureautique du menu KDE. Sélectionnez le type de serveur, tel que SLOX, GroupWise ou Exchange, dans la liste proposée, puis entrez l'adresse et les données d'authentification. L'assistant ajoute à Kontact les ressources disponibles.

Le module d'agenda peut être connecté à plusieurs agendas en même temps. Vous pouvez ainsi combiner un agenda personnel et un agenda professionnel, par exemple. Pour ajouter un agenda, cliquez sur *Add* (Ajouter), puis sélectionnez le type d'agenda souhaité. Renseignez les champs nécessaires.

Les cases à cocher situées en regard des agendas indiquent l'état d'activation de chaque agenda. Pour masquer un agenda sans le supprimer, désélectionnez la case correspondante. Cliquez sur *Remove* (Supprimer) pour supprimer de la liste l'agenda sélectionné.

12.6 Synchronisation des données avec un périphérique de poche

Vous pouvez synchroniser les données de Kontact avec des périphériques de poche, tels qu'un Palm. Des informations relatives à l'état de KPilot sont disponibles dans le résumé. Pour obtenir des informations sur la configuration et l'utilisation de KPilot, consultez le Chapitre 13, *Synchronisation d'un périphérique de poche avec KPilot* (p. 201).

12.7 Kontact pour les utilisateurs GroupWise

Si vous êtes habitué à travailler dans GroupWise, vous ne devriez pas avoir de problème à vous adapter à Kontact. Ces deux programmes ont en effet de nombreux concepts en commun et offrent, en grande partie, les mêmes services. Cette section aborde les principales différences terminologiques et fournit quelques conseils pour que les utilisateurs GroupWise profitent pleinement des possibilités de Kontact.

12.7.1 Différences terminologiques

Le tableau suivant répertorie quelques-unes des principales différences terminologiques entre Kontact et GroupWise.

Tableau 12.1 *Différences terminologiques entre Kontact et GroupWise*

GroupWise	Kontact
Appointments (Rendez-vous)	Events (Événements)

GroupWise	Kontact
Busy search (Plages disponibles)	Free/Busy (Disponibilités)
Notes	Journal entries (Entrées de journal)
Posted, nonposted items (Éléments publiés, non publiés)	Un événement sans participant est publié. Un événement qui comporte des participants est un élément envoyé.
Tâches	To-dos (Tâches)

12.7.2 Conseils pour les utilisateurs GroupWise

Cette section fournit aux utilisateurs GroupWise des conseils qui leur permettent d'appréhender certaines des différences existant entre GroupWise et Kontact.

Informations de contact

Vous pouvez ajouter vos contacts GroupWise Messenger et de messagerie à vos informations de contacts Kontact. Vous pouvez ensuite écrire un message électronique ou ouvrir une session de messagerie instantanée en utilisant ce contact ; pour ce faire, cliquez avec le bouton droit de la souris sur le nom qui apparaît dans la vue Contact.

Code de couleurs

Le codage des éléments GroupWise et provenant d'autres sources à l'aide de couleurs est très utile. Le code de couleurs vous permet de repérer facilement, parmi vos messages électroniques, contacts et autres informations, les éléments issus d'une source particulière.

Invitation de participants à des événements

Contrairement à GroupWise, Kontact ne vous inclut pas automatiquement en tant que participant dans les événements que vous planifiez. N'oubliez donc pas de vous inviter.

12.8 Pour plus d'informations

Kontact comprend une aide complète qui traite de tous ses composants. Pour y accéder, cliquez sur *Help (Aide)* → *Kontact Handbook (Manuel de Kontact)*. La page Web consacrée au projet, `http://www.kontact.org`, fournit également des informations utiles.

13 Synchronisation d'un périphérique de poche avec KPilot

Les périphériques de poche sont d'un usage très répandu auprès des utilisateurs qui ont besoin d'avoir constamment leurs plannings, listes des tâches et notes à portée de main. Dans la plupart des cas, les données accessibles doivent être les mêmes sur l'ordinateur et le périphérique de poche. C'est là qu'intervient KPilot. Cet outil permet de synchroniser les données du périphérique de poche avec celles utilisées par les applications KDE KAddressBook, KOrganizer et KNotes, qui font partie de la suite Kontact.

KPilot permet essentiellement de partager les données entre les applications d'un périphérique de poche et les programmes KDE correspondants. KPilot intègre ses propres visionneuse de mémos, visionneuse d'adresses et installateur de fichiers, mais ces utilitaires ne peuvent pas être utilisés en dehors de l'environnement KPilot. Seul l'installateur de fichiers n'a pas d'application KDE correspondante.

KPilot utilise des « conduits » pour établir la communication entre le périphérique de poche et les différents programmes du bureau. L'application KPilot elle-même gère l'ensemble des échanges de données entre les deux systèmes. Pour que vous puissiez utiliser une fonction particulière du périphérique de poche sur l'ordinateur, le conduit correspondant doit être activé et configuré. Pour la plupart, ces conduits sont destinés à interagir avec des programmes KDE déterminés et ne peuvent généralement pas être utilisés avec d'autres applications du bureau.

Le conduit de synchronisation horaire, qui est transparent pour l'utilisateur, fonctionne à l'arrière-plan lors de chaque synchronisation. Il ne doit être activé que sur les ordinateurs qui utilisent un serveur de synchronisation réseau pour corriger leur horloge interne.

Lors d'une synchronisation, les conduits sont activés l'un après l'autre pour le transfert de données. Il existe deux méthodes de synchronisation : une opération HotSync, qui ne synchronise que les données pour lesquelles des conduits ont été activés, et une opération de sauvegarde, qui effectue une sauvegarde complète de toutes les données stockées sur le périphérique de poche.

Comme certains conduits ouvrent un fichier pendant l'opération de synchronisation, le programme correspondant ne doit pas être en cours d'utilisation à ce moment. Ceci est surtout valable pour le programme KOrganizer.

13.1 Conduits utilisés par KPilot

Vous pouvez activer et configurer les conduits utilisés par KPilot après avoir sélectionné *Configuration → Configure KPilot (Configurer KPilot)*. Voici quelques-uns des principaux conduits :

Carnet d'adresses
Ce conduit est destiné à l'échange de données avec le carnet d'adresses du périphérique de poche. L'équivalent KDE pour la gestion de ces contacts est KAddressBook. Pour lancer l'application, passez par le menu principal ou utilisez la commande `kaddressbook`.

KNotes/Mémos
Ce conduit vous permet de transférer des notes créées avec KNotes dans l'application mémo du périphérique de poche. Pour lancer l'application KDE, passez par le menu principal ou utilisez la commande `knotes`.

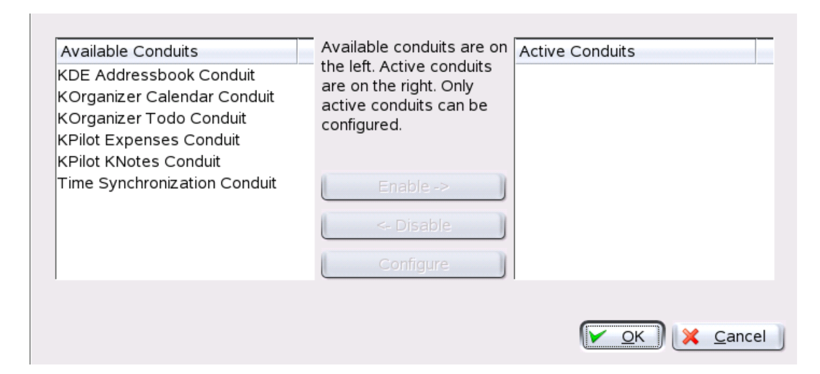
Agenda (KOrganizer)
Ce conduit gère la synchronisation de l'emploi du temps (rendez-vous) sur le périphérique de poche. KOrganizer est l'équivalent KDE de cette application.

Tâches (KOrganizer)
Ce conduit gère la synchronisation des tâches. KOrganizer est l'équivalent KDE de cette application.

Conduit de synchronisation horaire
Lorsque ce conduit est activé, l'horloge du périphérique de poche est réglée sur celle de l'ordinateur à chaque opération de synchronisation. Cet ajustement n'est judicieux

que si l'horloge de l'ordinateur est elle-même corrigée par un serveur de synchronisation à intervalles relativement fréquents.

Figure 13.1 *Boîte de dialogue de configuration avec les conduits disponibles*



13.2 Configuration de la connexion avec le périphérique de poche

Pour pouvoir utiliser KPilot, vous devez d'abord configurer la connexion avec le périphérique de poche. La configuration dépend du type de socle de synchronisation (station d'accueil) utilisé avec le périphérique de poche. Il en existe deux types : socles ou câbles de synchronisation USB et socles ou câbles de synchronisation série.

13.2.1 Configuration de la connexion depuis KPilot

La méthode la plus simple pour configurer la connexion consiste à utiliser l'assistant de configuration. Sélectionnez *Settings (Configuration)* → *Configuration Assistant (Assistant de configuration)* pour démarrer l'assistant. Indiquez tout d'abord votre nom d'utilisateur et le nom de l'unité à laquelle le périphérique de poche est connecté. L'assistant essaie de les détecter lui-même si vous sélectionnez l'option *Autodetect Handheld & Username (Détecter automatiquement le périphérique de poche et l'utilisateur)*. En cas d'échec de la reconnaissance automatique, reportez-vous à la Section 13.2.2, « Création d'un lien /dev/pilot » (p. 204).

Après avoir confirmé en cliquant sur *Next (Suivant)*, l'assistant vous invite à spécifier les applications à utiliser pour la synchronisation. Vous pouvez choisir la suite d'applications KDE (par défaut), Evolution ou aucune application. Une fois votre sélection effectuée, cliquez sur *Finish (Terminer)* pour fermer la fenêtre.

13.2.2 Création d'un lien /dev/pilot

La configuration de la connexion dépend du socle de synchronisation utilisé par le périphérique de poche : USB ou série. Le type de socle utilisé justifie la création ou la non-création d'un lien symbolique nommé `/dev/pilot`.

USB
: Normalement, les socles USB sont détectés automatiquement et il n'est pas nécessaire de créé le lien symbolique mentionné.

Série
: Dans le cas d'un socle série, vous devez également savoir à quel port série celui-ci est connecté. Les périphériques série portent le nom `/dev/ttyS?` ; la numérotation commence à `/dev/ttyS0` pour le premier port. Pour configurer la connexion avec un support relié au premier port série, tapez la commande suivante :

```
ln -s /dev/ttyS0 /dev/pilot
```

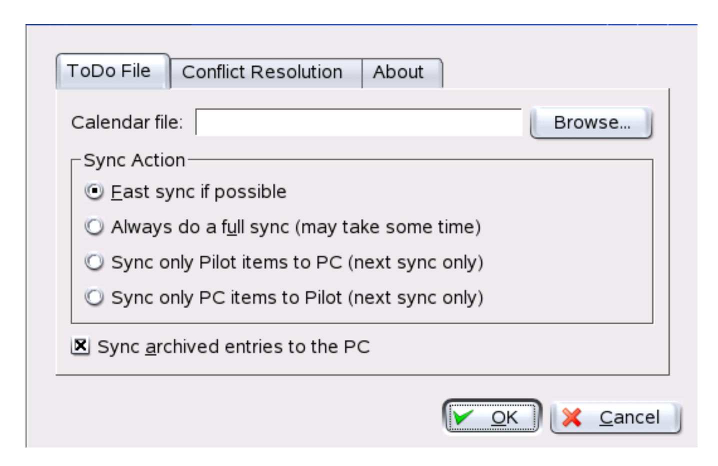
13.3 Configuration du conduit KAddressBook

Normalement, les paramètres du conduit KAddressBook sont prédéfinis de telle sorte que vous pouvez l'activer sans modifier la configuration par défaut. À l'issue de la première synchronisation, vous pouvez affiner la configuration du conduit. Voici quelques exemples : mesures à prendre en cas de conflits, mode d'enregistrement des bases de données de sauvegarde, caractéristiques d'affectation de certains champs du périphérique de poche aux entrées KAddressBook.

13.4 Gestion des tâches et des événements

Les tâches et les événements (rendez-vous) sont gérés sur le bureau KDE à l'aide de KOrganizer. Vous pouvez lancer cette application à partir du menu principal, à l'aide de la commande `korganizer` ou depuis Kontact. Après avoir activé les conduits KPilot pour l'agenda et les tâches, vous devez définir certaines options de configuration pour pouvoir les utiliser.

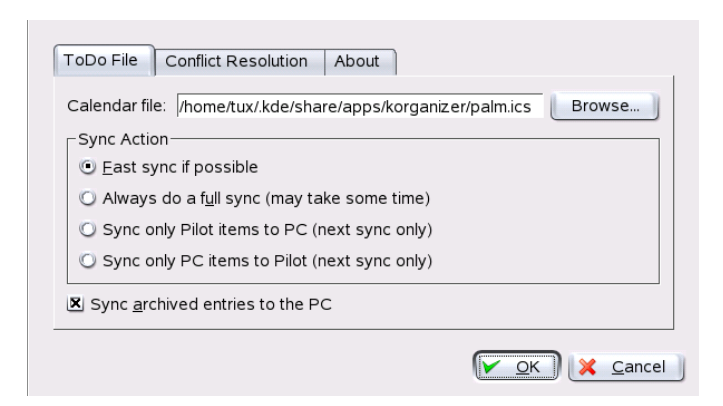
Figure 13.2 *Configuration de KPilot*



KOrganizer stocke ses fichiers dans le répertoire `~/.kde/share/apps/korganizer`. Notez toutefois que, comme le répertoire `.kde/` commence par un point, il est possible qu'il n'apparaisse pas dans la boîte de dialogue de sélection de fichiers. Dans ce cas, vous devez entrer manuellement le chemin complet ou activer explicitement l'affichage des fichiers cachés dans la boîte de dialogue. La touche de raccourci par défaut pour afficher les fichiers cachés est F8.

Dans le répertoire `~/.kde/share/apps/korganizer`, vous devez sélectionner un fichier qui sera reconnu comme un fichier agenda par KOrganizer. Dans cet exemple, il s'agit du fichier `palm.ics`. Dans le cas d'un utilisateur appelé `tux`, le chemin et le nom de fichier complet sera donc `/home/tux/.kde/share/apps/korganizer/palm.ics`, comme l'illustre la Figure 13.3, « Boîte de dialogue indiquant le chemin d'accès à un fichier agenda KOrganizer » (p. 206).

Figure 13.3 *Boîte de dialogue indiquant le chemin d'accès à un fichier agenda KOrganizer*

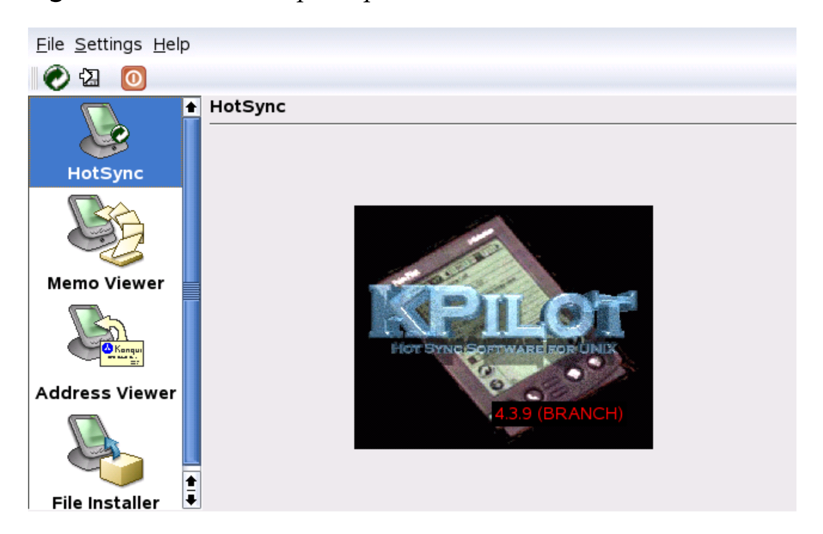


KOrganizer ne doit pas être en cours d'utilisation lors de l'échange de données avec le périphérique de poche. En effet, cela empêcherait KPilot de procéder à la synchronisation.

13.5 Utilisation de KPilot

La synchronisation de données entre les applications KDE et le périphérique de poche est très facile. Il suffit de démarrer KPilot et d'appuyer sur le bouton HotSync du socle ou du câble pour lancer l'opération de synchronisation.

Figure 13.4 *Fenêtre principale de KPilot*



13.5.1 Sauvegarde des données du périphérique de poche

Pour effectuer une sauvegarde complète, sélectionnez *File (Fichier)* → *Backup (Sauvegarde)*. La sauvegarde aura lieu lors de la prochaine synchronisation. Veillez ensuite à sélectionner à nouveau *File (Fichier)* → *HotSync*. Sinon, une sauvegarde complète, qui prend beaucoup de temps, sera à nouveau effectuée à la prochaine synchronisation.

Après une sauvegarde complète, toutes les copies des programmes et des bases de données du périphérique de poche sont stockées dans le répertoire `~/.kde/share/apps/kpilot/DBBackup/UTILISATEUR`, *`UTILISATEUR`* étant le nom de l'utilisateur enregistré sur le périphérique de poche.

Les deux visionneuses intégrées à KPilot permettent de consulter rapidement des adresses ou des mémos, mais elles ne sont pas adaptées à la gestion de ces données. Les applications KDE mentionnées plus haut conviennent beaucoup mieux pour la réalisation de ces tâches.

13.5.2 Installation de programmes sur le périphérique de poche

Le module *File Installer (Installateur de fichiers)* est un outil particulièrement utile pour installer des programmes sur le périphérique de poche. Normalement, ces programmes portent l'extension `.prc` et peuvent être démarrés immédiatement une fois chargés sur le périphérique de poche. Avant d'utiliser ces programmes supplémentaires, pensez à lire les licences d'utilisation et les instructions correspondantes.

13.5.3 Synchronisation des carnets d'adresses et des agendas

Utilisez l'utilitaire KDE MultiSynK pour synchroniser vos agendas et vos adresses. Tapez la commande `multisynk` pour démarrer l'utilitaire. Créez une paire de connecteurs (konnector) avant de synchroniser vos données. Choisissez l'option *File (Fichier)* → *New (Nouveau)* et sélectionnez vos connecteurs. Pour quitter l'utilitaire, cliquez sur *OK*.

Le nom apparaît dans la fenêtre principale. Pour procéder à la synchronisation avec votre périphérique de poche, sélectionnez *File (Fichier)* → *Sync (Synchroniser)*.

14 Utilisation de Beagle

Beagle est un outil de recherche qui indexe votre espace d'informations personnel pour vous aider à trouver ce que vous cherchez. Beagle permet de rechercher des documents, des messages électroniques, l'historique Web, des conversations de messagerie instantanée et ITC, du code source, des images, des fichiers de musique, des applications, etc.

Beagle prend en charge les sources de données suivantes :

- Système de fichiers
- Lanceurs d'applications
- Courrier électronique et carnet d'adresses Evolution
- Journaux de messagerie instantanée Gaim
- Pages Web Firefox (telles que vous les voyez)
- Aggregators Blam et Liferea RSS
- Notes avec Tomboy

Il prend également en charge les formats de fichier suivants :

- OpenOffice.org
- Microsoft Office (doc, ppt, xls)

- HTML
- PDF
- Images (jpeg, png)
- Audio (mp3, ogg, flac)
- AbiWord
- Rich Text Format (rtf)
- Texinfo
- Pages de manuel
- Code source (C, C++, C#, Fortran, Java, JavaScript, Pascal, Perl, PHP, Python)
- Texte brut

Beagle indexe automatiquement tout ce qui se trouve dans votre dossier personnel. Vous pouvez toutefois choisir d'exclure certains fichiers ou répertoires. Beagle inclut également un ensemble d'outils qui permettent de rechercher vos données.

14.1 Indexation des données

Le démon Beagle (`beagled`) effectue automatiquement toute l'indexation. Par défaut, l'ensemble de votre dossier personnel est indexé. Beagle détecte les changements effectués dans votre dossier personnel et réindexe les données en conséquence.

- Les fichiers sont immédiatement indexés lors de leur création, ils sont réindexés lorsqu'ils sont modifiés, et ils sont ignorés lorsqu'ils sont supprimés.
- Les messages électroniques sont indexés à leur arrivée.
- Les conversations IM sont indexées à mesure que vous discutez, ligne après ligne.

L'indexation de vos données nécessite une puissance informatique importante, mais le démon Beagle tente de rester aussi discret que possible. Il contient un planificateur qui

hiérarchise les tâches et contrôle l'utilisation de l'unité centrale, selon que vous utilisez votre station de travail de façon active ou non.

14.1.1 Comment empêcher l'indexation des fichiers et des répertoires

Si vous souhaitez empêcher l'indexation d'un répertoire (et de tous ses sous-répertoires), créez un fichier vide nommé `.noindex` et placez-le dans le répertoire. Vous pouvez ajouter une liste de fichiers et de répertoires au fichier `.noindex` pour empêcher l'indexation de ces derniers. Les jokers sont autorisés dans le fichier `.noindex`.

Vous pouvez également placer un fichier `.neverindex` dans votre dossier personnel avec la liste des fichiers qui ne doivent jamais être indexés. Les jokers sont également autorisés dans ce fichier. Utilisez les mêmes jokers que pour `glob` (par exemple, `f*le ??.txt`). Vous pouvez également utiliser des expressions régulières plus puissantes en ajoutant une barre oblique normale avant et après (par exemple, `/fichier.* .txt/`). Pour plus d'informations, consultez le site Web glob-UNIX (http://docs.python.org/lib/module-glob.html).

14.1.2 Indexation manuelle

Beagle est doté d'un système efficace permettant de déterminer quand à quel moment vos fichiers. Il tente en outre de ne pas interférer avec les autres applications en cours d'exécution. Il synchronise volontairement son indexation en fonction de la charge et selon que votre système est actif ou non, de manière à ne pas perturber votre utilisation du bureau. Toutefois, si vous souhaitez indexer immédiatement votre dossier personnel, entrez la commande suivante dans une fenêtre de terminal avant d'exécuter Beagle :

```
export BEAGLE_EXERCISE_THE_DOG=1
```

14.1.3 Vérification de l'état de votre index

Beagle inclut les commandes suivantes pour voir l'état d'indexation en cours :

`beagle-index-info`
Affiche le nombre et le type de documents ayant été indexés.

beagle-status
Affiche la tâche courante du démon Beagle (sur une base continue).

14.2 Recherche de données

Beagle propose les outils suivants pour rechercher les données que vous avez indexées.

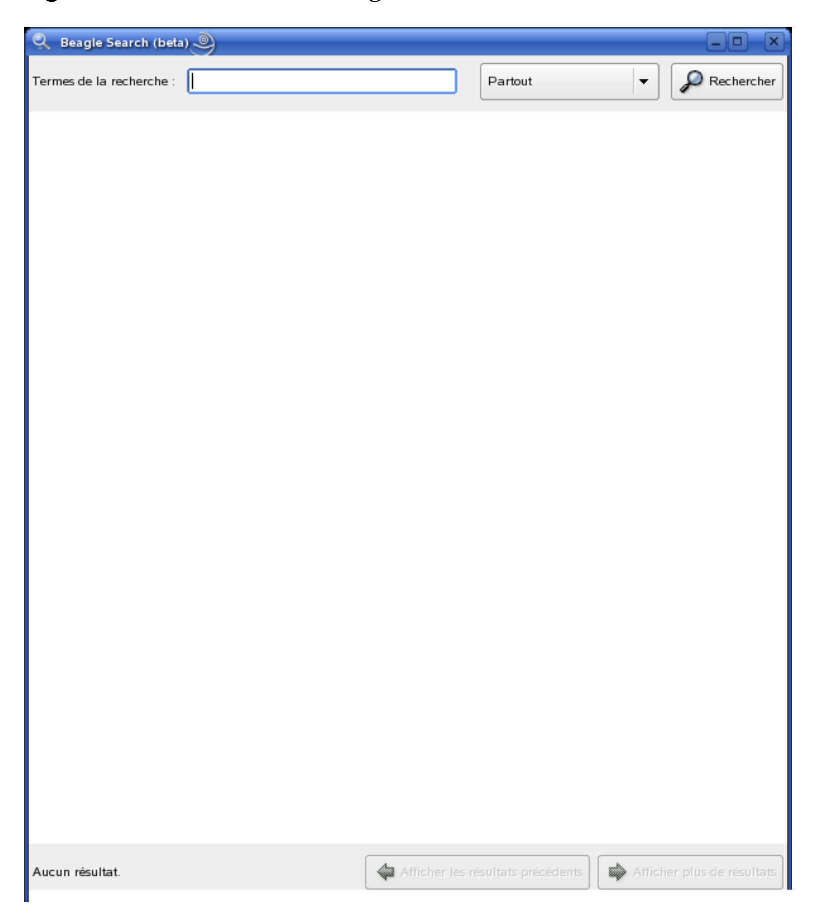
14.2.1 Best

Best (Bleeding Edge Search Tool) est un outil graphique qui recherche vos informations indexées. Best n'interroge pas directement l'index ; il transmet les termes de la recherche au démon Beagle, qui renvoie les correspondances éventuelles à Best. Best affiche ensuite les résultats et permet d'effectuer des actions sur les objets trouvés.

Pour ouvrir Best dans KDE, cliquez sur *K Menu (Menu K)* → *System (Système)* → *File System (Système de fichiers)* → *Beagle Search (Recherche Beagle)*. Pour ouvrir Best dans KDE, cliquez sur *K Menu (Menu K)* → *System (Système)* → *File System (Système de fichiers)* → *Beagle Search (Recherche Beagle)*.

Pour utiliser Best, tapez simplement votre texte dans la zone de saisie située en haut et appuyez sur Entrée ou cliquez sur *Find (Rechercher)*. Best interroge vos fichiers indexés et renvoie les résultats.

Figure 14.1 Recherche Beagle



Vous pouvez utiliser la liste des résultats pour ouvrir un fichier, envoyer un fichier par courrier électronique, envoyer un message instantané, répondre à un fichier, transférer un fichier ou afficher un fichier dans votre gestionnaire de fichiers. Les options disponibles pour chaque fichier dépendent de son type.

Vous pouvez également utiliser *Anywhere (N'importe où)* pour limiter votre recherche aux fichiers d'un emplacement particulier, par exemple votre carnet d'adresses ou des pages Web, ou pour n'afficher qu'un type spécifique de fichier dans votre liste de résultats.

14.2.2 beagle-query

Beagle est doté d'un outil de ligne de commande que vous pouvez utiliser pour effectuer des recherches dans votre index Beagle. Pour utiliser cet outil, entrez la commande suivante dans une fenêtre de terminal :

```
beagle-querysearch
```

Remplacez *search* par le texte à rechercher pour que l'outil beagle-query renvoie des résultats. Cette commande permet d'utiliser des jokers.

Utilisez `beagle-query --verbose search` pour afficher des informations détaillées concernant les résultats de la recherche.

Applications graphiques

Appareils photo numériques et Linux 15

À partir du moment où vous disposez des bons outils, gérer les photos stockées sur votre appareil photo est un jeu d'enfant. Linux propose plusieurs utilitaires pratiques pour trier et organiser les photos. Il s'agit des utilitaires gphoto2, Konqueror, Digikam et f-spot.

La liste complète des appareils photo pris en charge est disponible sur la page Web `http://www.gphoto.org/proj/libgphoto2/support.php`. Si gphoto2 est installé, récupérez cette liste à l'aide de la commande `gphoto2 --list-cameras`. Pour obtenir des informations sur les commandes disponibles, utilisez `gphoto2 --help`.

ASTUCE: Appareils photo non pris en charge

Si vous ne trouvez pas votre appareil photo dans la liste affichée par gphoto, ne vous inquiétez pas. Votre appareil photo peut tout à fait être pris en charge en tant que périphérique USB Mass Storage. Pour plus d'informations, reportez-vous à la Section 15.2, « Accès à l'appareil photo » (p. 218).

15.1 Connexion avec l'appareil photo numérique

La manière la plus rapide et facile de connecter un appareil photo numérique à un ordinateur est d'utiliser un câble et un port USB, pour autant que le noyau, l'appareil et

l'ordinateur prennent en charge l'USB. Le noyau SUSE standard assure cette prise en charge. Un câble adéquat est également requis.

Connectez l'appareil au port USB et mettez l'appareil sous tension. Il se peut que vous deviez mettre votre appareil dans un mode spécial pour le transfert de données. Pour savoir comment faire, consultez le manuel de votre appareil.

15.2 Accès à l'appareil photo

Il existe trois possibilités pour accéder aux images stockées sur un appareil photo. Le choix dépend de votre appareil photo et du protocole qu'il prend en charge. Il s'agit le plus souvent du protocole USB Mass Storage, géré par le système d'enfichage à chaud, ou du protocole PTP (également appelé PictBridge). Certains modèles d'appareils photo ne fonctionnent avec ni l'un ni l'autre. Leur prise en charge est possible via gphoto2, qui comprend des pilotes spécifiques.

Le plus simple est lorsque votre appareil photo prend en charge le protocole USB Mass Storage. Si vous n'êtes pas sûre de cette possibilité, reportez-vous à la documentation de votre appareil photo. Certains appareils prennent en charge deux protocoles (aussi bien le protocole USB Mass Storage que le protocole PTP, par exemple). Malheureusement, d'autres modèles passent par un protocole propriétaire pour communiquer, ce qui peut vous compliquer la tâche. Si votre appareil photo ne prend pas en charge le protocole USB Mass Storage ni le protocole PTP, les descriptions suivantes ne sont pas applicables à votre cas. Essayez la commande `gphoto2 --list-cameras` et reportez-vous aux informations du site `http://www.gphoto.org/`.

Si votre appareil photo peut fonctionner avec le protocole USB Mass Storage, sélectionnez cette option. Une fois que vous l'avez connecté au port USB de votre ordinateur et mis sous tension, le système d'enfichage à chaud le détecte. Ce système se charge de monter automatiquement ce périphérique pour en faciliter l'accès. Une fois le montage réussi, un petit appareil photo s'affiche sur le bureau KDE.

Une fois l'appareil photo monté, un nouveau répertoire est créé sous `/media`. Il commence par les lettres `usb`, suivies d'une longue série de chiffres. Chaque fabricant et chaque produit est associé à un numéro unique : ainsi, lorsque vous branchez un périphérique sur votre ordinateur, il porte toujours le même nom. En fonction des autres dispositifs connectés au bus USB, il existe différentes entrées. Le seul problème à résoudre est de retrouver l'entrée correspondant à votre appareil photo. Essayez de développer la structure de l'un de ces répertoires (`DCIM/`*`xxx`*) pour en afficher les

éléments. Chaque appareil photo possède une arborescente différente : il n'y a donc pas de règle générale. Si des fichiers JPEG s'affichent dans un répertoire, c'est probablement celui que vous recherchez.

Le répertoire approprié trouvé, vous pouvez copier, déplacer ou supprimer les fichiers de votre appareil photo à l'aide d'un gestionnaire de fichiers (Konqueror, par exemple) ou de commandes de shell simples (reportez-vous à la Section 27.3, « Commandes Linux importantes » (p. 435) et au guide de *référence*).

15.3 Utilisation de Konqueror

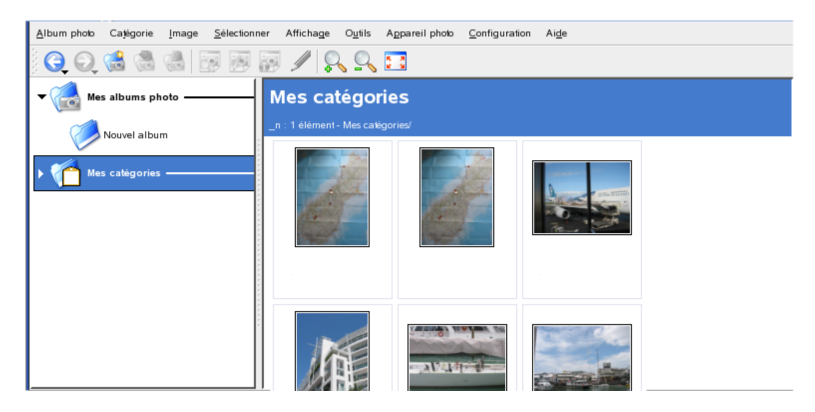
Les utilisateurs KDE peuvent facilement accéder à leur appareil photo numérique grâce à l'interface familière de Konqueror. Connectez votre appareil au port USB. Un petit appareil apparaît sur le bureau. Cliquez dessus pour ouvrir l'appareil photo dans Konqueror. Vous pouvez également taper l'URL`camera:/` de l'appareil dans Konqueror. Développez la structure de répertoires de l'appareil photo jusqu'à voir les fichiers. Utilisez les fonctions habituelles de gestion des fichiers de Konqueror afin de copier les fichiers selon vos besoins. Pour plus d'informations sur l'utilisation de Konqueror, reportez-vous au Chapitre 3, *Le navigateur Web Konqueror* (p. 79).

15.4 Utilisation de Digikam

Digikam est un programme KDE qui permet de télécharger les photos stockées sur un appareil numérique. La première fois que vous l'exécutez, Digikam vous demande de lui indiquer l'emplacement de stockage de votre album photo. Si vous entrez un répertoire qui contient déjà une collection de photos, Digikam traite chaque sous-dossier comme un album.

Au démarrage, Digikam présente une fenêtre divisée en deux sections : vos albums s'affichent à gauche et les photos de l'album en cours à droite. (voir Figure 15.1, « Fenêtre principale de Digikam » (p. 220)).

Figure 15.1 *Fenêtre principale de Digikam*



15.4.1 Configuration de votre appareil photo

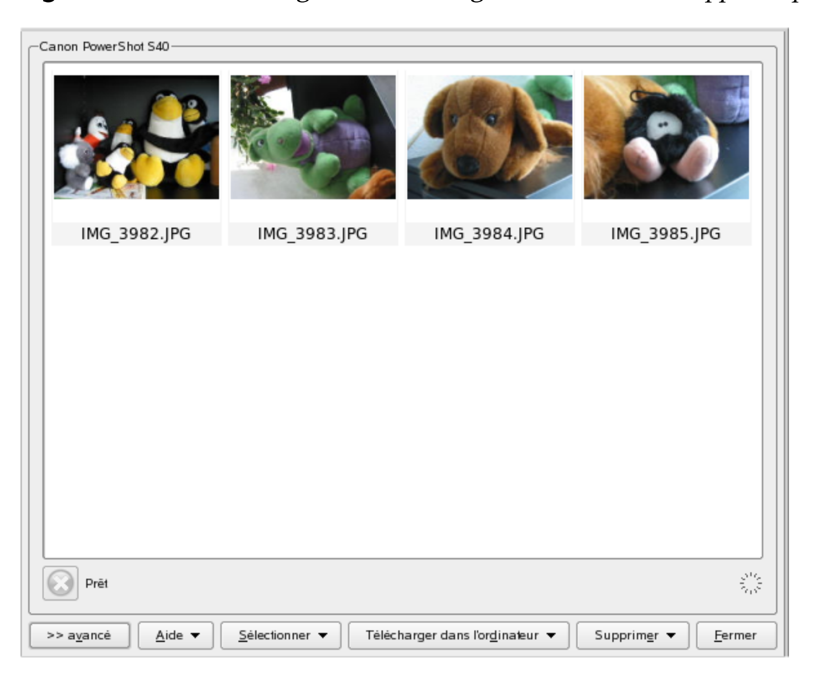
Pour configurer un appareil photo dans Digikam, sélectionnez *Camera (Appareil photo)* → *Add Camera (Ajouter appareil photo)*. Tout d'abord, essayez de détecter automatiquement l'appareil en cliquant sur *Détection automatique*. Si cette tentative n'aboutit pas, cliquez sur *Add (Ajouter)* pour rechercher votre modèle dans la liste. Si le modèle de votre appareil photo n'est pas inclus dans cette liste, essayez un ancien modèle ou utilisez l'option *USB/IEEE mass storage camera (Appareil photo de stockage de masse USB/IEEE)*. Cliquez sur *OK* pour confirmer.

15.4.2 Téléchargement des images stockées sur votre appareil photo

Une fois votre appareil photo correctement configuré, connectez-vous à lui via le menu *Camera (Appareil photo)* et le nom que vous avez entré dans la boîte de dialogue à la Section 15.4.1, « Configuration de votre appareil photo » (p. 220). Digikam ouvre une fenêtre et commence à télécharger les miniatures qu'il affiche, comme l'illustre la Figure 15.2, « Téléchargement des images stockées sur un appareil photo » (p. 221). Cliquez avec le bouton droit de la souris sur une image pour ouvrir un menu contextuel proposant des options pour *afficher* cette image, pour afficher ses *propriétés* ou ses *informations EXIF*, ou pour la *télécharger* ou la *supprimer*. Grâce à l'option *Advanced*

(Avancé), sélectionnez des options de changement de nom, ainsi que le mode de traitement des informations fournies par l'appareil photo (EXIF).

Figure 15.2 *Téléchargement des images stockées sur un appareil photo*



Les options de changement de nom peuvent être très pratiques si votre appareil photo n'utilise pas des noms de fichier explicites. Vous pouvez laisser Digikam renommer automatiquement vos photos. Indiquez un préfixe unique et, éventuellement, une date, une heure et un numéro de séquence. Digikam s'occupe du reste.

Sélectionnez toutes les photos à télécharger de l'appareil en appuyant sur le bouton gauche de la souris ou en cliquant sur les différentes photos tout en maintenant la touche Ctrl enfoncée. Les photos sélectionnées apparaissent avec les couleurs inversées. Cliquez sur *Download (Télécharger)*. Sélectionnez la cible dans la liste ou créez un album cible à l'aide de l'option *New Album (Nouvel album)*. Le système vous suggère alors automatiquement un nom de fichier comprenant la date du jour. Confirmez en cliquant sur *OK*, ce qui lance le processus de téléchargement.

15.4.3 Obtention d'informations

L'obtention d'informations relatives à une photo n'est pas difficile. Un bref résumé s'affiche dans une info-bulle lorsque vous placez le pointeur de la souris sur la miniature. Pour plus d'informations, cliquez avec le bouton droit de la souris sur la photo et choisissez *Properties (Propriétés)* dans le menu. Une boîte de dialogue s'ouvre. Elle comporte trois onglets : *General (Général)*, *EXIF* et *Histogram (Histogramme)*.

L'onglet *General (Général)* indique le nom, le type et le propriétaire de l'image, ainsi que d'autres informations de base. Les informations les plus intéressantes se trouvent dans l'onglet *EXIF*. L'appareil photo stocke des métadonnées pour chaque photo. Digikam lit ces propriétés et les affiche dans cette liste. Vous y trouverez le temps d'exposition, des dimensions en pixels, etc. Pour plus d'informations sur l'entrée sélectionnée dans la liste, appuyez sur Shift + F1. Une petite info-bulle s'affiche. Le dernier onglet, *Histogram (Histogramme)*, propose des informations d'ordre statistique.

15.4.4 Gestion des albums

Digikam crée un dossier *My Albums (Mes albums)* par défaut, qui sert à collecter toutes vos photos. Vous pouvez ensuite les enregistrer dans des sous-dossiers. Vous pouvez trier les albums en fonction de la disposition des répertoires, du nom de collection qui a été défini dans les propriétés de l'album ou de la date de création initiale des albums (vous pouvez également modifier cette date dans les propriétés de chaque album).

Pour créer un album, vous avez plusieurs possibilités :

- Téléchargez les nouvelles photos stockées sur l'appareil photo.
- Créez un album en cliquant sur le bouton *New Album (Nouvel album)* de la barre d'outils.
- Importez un dossier de photos enregistré sur votre disque dur. Sélectionnez pour cela *Album → Import (Importer) → Import Folders (Importer des dossiers)*.
- Cliquez avec le bouton droit de la souris sur le dossier *My Albums (Mes albums)* et sélectionnez *New Album (Nouvel album)*.

Sélectionnez la méthode de votre choix pour créer un album et une boîte de dialogue apparaît. Attribuez un titre à votre album. Vous pouvez éventuellement choisir une

collection, insérer des commentaires et sélectionner une date d'album. La collection permet d'organiser sous un intitulé commun différents albums. Cet intitulé sert lorsque vous sélectionnez *View (Afficher)* → *Sort Albums (Trier les albums)* → *By Collection (Par collection)*. Le commentaire s'affiche dans la bannière en haut de la fenêtre principale. La date de l'album sert lorsque vous sélectionnez *View (Afficher)* → *Sort Albums (Trier les albums)* → *By Date (Par date)*.

Digikam utilise la première photo de l'album comme icône d'aperçu dans la liste *My Albums (Mes albums)*. Pour en sélectionner une autre, cliquez avec le bouton droit de la souris sur la photo correspondante et sélectionnez *Set as Album Thumbnail (Définir en tant que miniature d'album)* dans le menu contextuel.

15.4.5 Gestion des onglets

La gestion d'un grand nombre de photographies différentes dans plusieurs albums peut parfois se révéler être une tâche complexe. Pour organiser des photographies individuelles, Digikam propose le système *My Tag (Mes étiquettes)*.

Exemple : vous avez pris à différentes occasions des photos de votre ami John et vous voulez collecter toutes ces images, indépendamment de votre album. Ce système permet de retrouver très facilement toutes ces photos. Tout d'abord, cliquez sur *My Tags (Mes étiquettes)* → *People (Gens)* pour créer une nouvelle étiquette. Dans le menu contextuel, choisissez *New Tag (Nouvelle étiquette)*. Dans la boîte de dialogue qui s'affiche, entrez le titre *John* et, éventuellement, définissez une icône. Cliquez sur *OK* pour confirmer.

Une fois l'étiquette créée, assignez-lui les images de votre choix. Accédez à chaque album et sélectionnez les photos respectives. Cliquez avec le bouton droit de la souris et, dans le menu contextuel, choisissez *Assign Tag (Assigner étiquette)* → *People (Gens)* → *John*. Vous pouvez également faire glisser les photos vers le nom de l'étiquette dans la zone *My Tags (Mes étiquettes)*. Répétez cette opération autant de fois que nécessaire, avec tous les albums concernés. Affichez toutes les images en cliquant sur *My Tags (Mes étiquettes)* → *People (Gens)* → *John*. Vous pouvez assigner plusieurs étiquettes à chaque photo.

La modification des étiquettes et des commentaires peut être fastidieuse. Pour simplifier cette tâche, cliquez avec le bouton droit de la souris sur une photo et sélectionnez *Edit Comments & Tags (Modifier les commentaires et les étiquettes)*. Une boîte de dialogue s'ouvre, avec un aperçu, un champ de commentaire et la liste des étiquettes. À cette étape, vous pouvez insérer toutes les étiquettes nécessaires et ajouter un commentaire.

Cliquez sur les boutons *Forward (Suivant)* et *Back (Précédent)* pour faire défiler les photos de votre album. Cliquez sur *Apply (Appliquer)* pour enregistrer vos modifications, puis sur *OK* pour quitter cette boîte de dialogue.

15.4.6 Exportation des collections d'images

Digikam propose plusieurs options d'exportation qui permettent d'archiver et de publier vos collections d'images personnelles. Vous pouvez archiver vos photos sur un CD ou un DVD (via k3b), ou les exporter au format HTML, éventuellement dans une galerie distante.

Pour enregistrer votre collection d'images sur un CD ou un DVD, procédez comme suit :

1. Sélectionnez *File (Fichier) → Export (Exporter) → Archive to CD/DVD (Archiver sur CD/DVD)*.

2. Effectuez vos réglages dans la boîte de dialogue *Create CD/DVD Archive (Créer archive CD/DVD)* à l'aide de ses différents sous-menus. Vos réglages terminés, cliquez sur *OK* pour lancer la gravure.

    a. *Sélection* : Déterminez la partie de votre collection à archiver en sélectionnant des albums et des onglets.

    b. *HTML Interface (Interface HTML)* : indiquez si votre collection d'images doit être accessible via une interface HTML et si une fonctionnalité d'exécution automatique doit être ajoutée à votre archive sur CD/DVD. Définissez un titre et une image de sélection, la police et les propriétés d'arrière-plan.

    c. *Media Volume Descriptor (Descripteur de volume de support)* : modifiez les paramètres de description du volume, si nécessaire.

    d. *Media Burning (Gravure de supports)* : réglez les options de gravure en fonction de vos besoins, si nécessaire.

Pour exporter votre collection d'images au format HTML, procédez comme suit :

1 Sélectionnez *File (Fichier) → Export (Exporter) → HTML Export (Export HTML)*.

2 Utilisez les différents sous-menus pour régler les paramètres dans *Create Image Galleries (Créer galeries d'images)* en fonction de vos besoins. Cette opération terminée, cliquez sur *OK* pour lancer la création de la galerie.

   a *Sélection* : Déterminez la partie de votre collection à archiver en sélectionnant des albums et des onglets.

   b *Look (Aspect)* : définissez le titre et l'aspect de votre galerie HTML.

   c *Album* : déterminez l'emplacement de la galerie sur le disque, ainsi que la taille des images, leur compression, leur format et la quantité de métadonnées affichées dans la galerie finale.

   d *Thumbnails (Miniatures)* : comme pour les images cibles, indiquez la taille, la compression et le type de fichier des images miniatures utilisées lors de la navigation dans la galerie.

Pour exporter votre collection dans une galerie d'images externe sur Internet, procédez comme suit :

1 Créez un compte sur le site Web externe où sera conservée votre galerie.

2 Sélectionnez *File (Fichier) → Export (Exporter) → Export to Remote Gallery (Exporter vers galerie distante)*, puis indiquez l'URL, le nom d'utilisateur et le mot de passe du site externe lorsqu'ils vous sont demandés.

   Digikam établit une connexion avec le site indiqué et ouvre une nouvelle fenêtre intitulée *Gallery Export (Exportation galerie)*.

3 Déterminez l'emplacement de votre nouvel album dans la galerie.

4 Cliquez sur *New Album (Nouvel album)* et indiquez les informations demandées par Digikam.

5 Téléchargez les images dans le nouvel album à l'aide de l'option *Add Photos (Ajouter photos)*.

15.4.7 Outils pratiques

Digikam propose plusieurs outils qui permettent de simplifier certaines tâches. Ils sont accessibles depuis le menu *Tools (Outils)*. Voici un échantillon de ces outils disponibles.

Création d'un calendrier

Si vous voulez faire plaisir à quelqu'un, un calendrier personnalisé peut être un joli cadeau. Accédez au menu *Tools (Outils)* → *Create Calendar (Créer calendrier)*. La boîte de dialogue d'un Assistant s'ouvre. Elle ressemble à celle de la Figure 15.3, « Création d'un modèle de calendrier » (p. 226).

Figure 15.3 *Création d'un modèle de calendrier*

Personnalisez les paramètres (format de la page, positionnement de l'image, police, etc.), puis confirmez-les en cliquant sur *Next (Suivant)*. À cette étape, vous pouvez entrer l'année et sélectionner les images à utiliser. Cliquez de nouveau sur *Next (Suivant)*. Un résumé s'affiche. Le dernier bouton *Next (Suivant)* permet d'ouvrir la boîte de dialogue d'impression de KDE. Vous pouvez à cette étape décider d'afficher un aperçu, d'enregistrer au format PDF ou de tout simplement imprimer directement votre document.

Recherche de photos en double

Parfois, vous photographiez des scènes semblables plusieurs fois et ne voulez en conserver que les meilleurs clichés. Le plug-in *Find Duplicate (Rechercher les doublons)* est l'outil idéal pour accomplir cette tâche.

Accédez au menu *Tools (Outils)* → *Find Duplicate Images (Rechercher les photos en double)*. Sélectionnez les albums ou les étiquettes à gérer. Dans la zone *Method & Cache (Méthode et cache)*, choisissez une méthode de recherche, en fonction de vos priorités (précision ou rapidité). Lorsque vous confirmez vos paramètres en cliquant sur *OK*, Digikam lance la recherche.

S'il découvre des doublons, il affiche les résultats dans une fenêtre comme celle de la Figure 15.4, « Résultats de la recherche » (p. 227). Décidez quelles images supprimer en cochant les cases correspondantes, puis cliquez sur *Delete (Supprimer)*. Cliquez sur *Close (Fermer)* pour quitter cette fenêtre.

Figure 15.4 *Résultats de la recherche*

Processus par lots

Digikam propose également des processus par lots qui permettent d'exécuter une tâche spécifique sur un grand nombre de fichiers. Il peut s'agir de changement de nom, de conversion, de redimensionnement et de bien d'autres tâches encore. Pour ce faire, accédez au menu *Tools (Outils) → Batch Processes (Processus par lots)*.

15.4.8 Affichage et édition de base des images dans Digikam

Digikam comprend son propre programme de base d'affichage et d'édition des images. Il s'ouvre automatiquement si vous double-cliquez sur la miniature d'une image.

Utilisez cet outil pour effectuer certaines tâches d'édition de base sur les images que vous venez de télécharger depuis votre appareil photo. Vous pouvez rogner, faire pivoter ou inverser l'image, effectuer certains réglages couleur de base, appliquer différents filtres colorés (par exemple, pour exporter en noir et blanc une image couleur) et réduire efficacement l'effet « yeux rouges » sur les portraits.

Les menus les plus importants sont les suivants :

Image

Le menu *Edit Comments & Tags (Modifier les commentaires et les étiquettes)* permet d'entrer des commentaires pour une image particulière et de lui assigner une étiquette (catégorie). Le menu *Properties (Propriétés)* ouvre une fenêtre comportant trois onglets avec des informations générales, des informations EXIF et l'histogramme de cette image.

Fix (Corriger)

Ce menu contient certaines des fonctions d'édition souvent utilisées en photographie numérique. Le menu *Colors (Couleurs)* affiche un sous-menu qui permet de modifier tous les paramètres de couleur de base. Vous pouvez également rendre l'image plus floue ou plus nette, dans sa totalité ou en partie seulement, en fonction de la zone vous sélectionnez. Pour réduire l'effet « yeux rouges » sur un portrait, sélectionnez grosso modo la zone des yeux sur le visage. Pour ce faire, il suffit de cliquer et de maintenir le bouton gauche de la souris enfoncé tout en étendant graduellement la zone de sélection. Sélectionnez ensuite *Red Eye Reduction (Réduction de l'effet yeux*

rouges), puis choisissez une réduction légère ou « agressive » (appuyée) selon que vous avez sélectionné toute une zone ou juste les yeux.

Transform (Transformer)

Le menu *Transform (Transformer)* propose des fonctions pour rogner, faire pivoter, inverser et redimensionner l'image. Vous pouvez également utiliser l'option *Aspect Ratio Crop (Rogner l'aspect)* pour rogner en fonction d'un rapport hauteur/largeur fixe.

Filtres

Si vous avez besoin de transformer vos clichés couleur en noir et blanc ou si vous voulez donner un aspect vieilli à vos photos, choisissez l'une des options d'exportation du menu *Filters (Filtres)*.

Une description plus détaillée de cet outil est disponible dans l'aide en ligne de Digikam, dans la rubrique relative à l'*éditeur d'images de Digikam*, accessible via le bouton *Help (Aide)* de la barre de menus de Digikam.

ASTUCE: Traitement avancé des images

Vous pouvez éditer des images de façon professionnelle dans GIMP. Pour plus d'informations sur GIMP, reportez-vous au Chapitre 17, *Manipulation des graphiques au moyen de GIMP* (p. 247).

15.5 Utilisation de f-spot

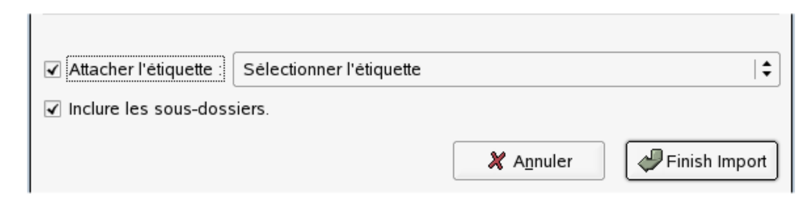
f-spot est un outil de gestion pour votre collection d'images numériques, conçu pour le bureau GNOME. Il permet d'assigner différentes étiquettes à vos images afin de les classer par catégories. Il propose également plusieurs options d'édition soignée des images.

La première fois que vous exécutez f-spot, indiquez-lui les emplacements à partir desquels importer les images dans votre collection f-spot. Si vous avez déjà une collection d'images enregistrée sur votre disque dur, entrez le chemin d'accès au répertoire correspondant et, éventuellement, incluez des sous-dossiers. f-spot importe ces images dans sa base de données.

ASTUCE: Application d'une étiquette aux images pendant l'importation

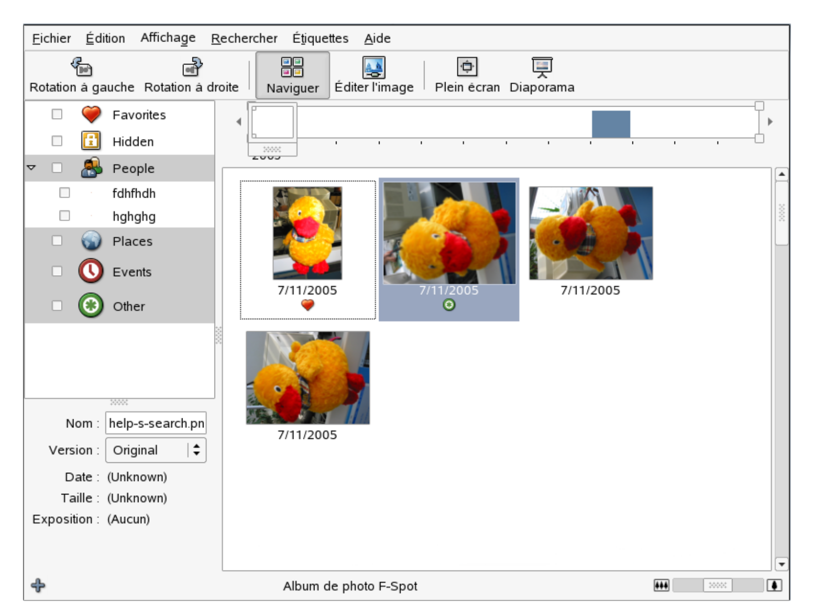
Si toutes les images que vous importez appartiennent à la même catégorie, vous pouvez leur associer l'étiquette appropriée pendant l'importation. Sélectionnez *Attach Tag (Attacher étiquette)* et choisissez l'étiquette correspondante dans le menu déroulant.

Figure 15.5 *Importation d'images dans f-spot*



La fenêtre principale de f-spot est divisée en trois zones principales. Les catégories, les étiquettes et les informations détaillées relatives aux images sélectionnées s'affichent sur le côté, à gauche. Une image miniature de chaque photo correspondant à l'étiquette ou à la catégorie sélectionnée s'affiche dans la partie droite de la fenêtre. Si vous n'avez pas fait de sélection, c'est la collection complète qui s'affiche.

Figure 15.6 Fenêtre principale de f-spot



Une barre de menus tout en haut de la fenêtre permet d'accéder aux menus principaux. Au dessous, une barre d'outils propose plusieurs fonctions illustrées par une icône correspondante :

Rotate (Left or Right) (Rotation gauche ou droite)
Utilisez ce raccourci pour changer l'orientation d'une image.

Browse (Parcourir)
Le mode *Browse (Parcourir)* permet d'afficher et de rechercher des images dans la totalité de votre collection ou dans des sous-ensembles étiquetés de cette collection. Vous pouvez également utiliser la ligne de temps pour rechercher des images en fonction de leur date de création.

Edit Image (Modifier l'image)
Ce mode permet de sélectionner une image et de lui appliquer des traitements d'image de base. Pour plus d'informations, reportez-vous à la Section 15.5.6, « Traitement de base des images dans f-spot » (p. 236).

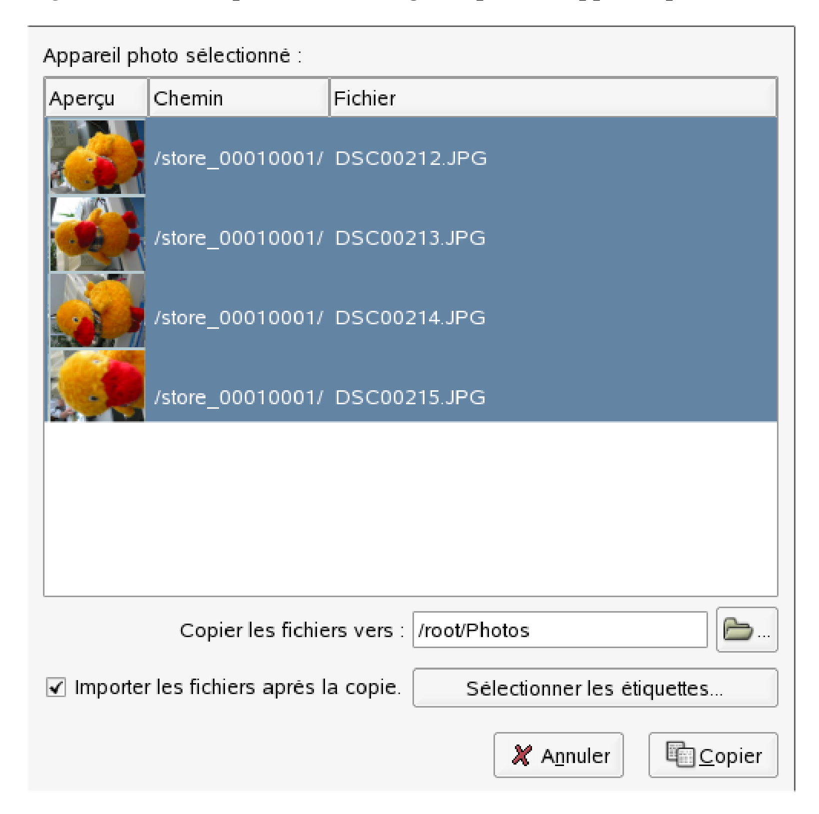
Fullscreen (Plein écran)
Permet de choisir le mode d'affichage plein écran.

Slideshow (Diaporama)
Lance un diaporama.

15.5.1 Téléchargement des images stockées sur votre appareil photo

Importez de nouvelles images depuis votre appareil photo branché sur le port USB de votre ordinateur, à l'aide du menu *File (Fichier)* → *Import from Camera (Importer depuis l'appareil photo)*. Le type de l'appareil photo est détecté automatiquement.

Figure 15.7 *Importation d'images depuis un appareil photo*



f-spot lance la fenêtre d'aperçu dans laquelle s'affichent les images qui peuvent être téléchargées depuis l'appareil photo. Les fichiers sont copiés dans répertoire cible indiqué

via l'option *Copy Files to (Copier les fichiers vers)*. Si l'option *Import files after copy (Importer les fichiers après la copie)* est sélectionnée, toutes les images copiées à partir de l'appareil photo sont automatiquement importées dans la base de données de f-spot. L'application d'étiquettes peut être effectuée au cours de l'importation, si vous sélectionnez l'étiquette appropriée à l'aide de *Select Tags (Sélectionner les étiquettes)*. Si vous ne voulez pas importer toutes les images stockées sur votre appareil photo dans votre base de données, il suffit de désélectionner celles que vous ne voulez pas dans la fenêtre d'aperçu.

15.5.2 Obtention d'informations

Lorsque vous sélectionnez une image, des informations statistiques de base la concernant s'affichent dans la partie inférieure gauche de la fenêtre. Parmi ces informations, se trouvent le nom du fichier, sa version (copie ou image d'origine), sa date de création, sa taille et l'exposition utilisée lors de la création de cette image spécifique. Affichez les données EXIF associées au fichier d'image à l'aide du menu *View (Afficher) → EXIF Data (Données EXIF)*.

15.5.3 Gestion des onglets

Utilisez les étiquettes pour classer vos images par catégories afin de créer des sous-ensembles gérables de votre collection. Si, par exemple, vous voulez ordonner un tant soit peu votre collection de portraits de vos proches, procédez comme suit :

1. Dans f-spot, sélectionnez le mode *Browse (Parcourir)*.

2. Dans l'encadré de gauche de la fenêtre f-spot, sélectionnez la catégorie *People (Gens)*, cliquez dessus avec le bouton droit de la souris, puis choisissez *Create New Tag (Créer de nouvelles étiquettes)*. Ces nouvelles étiquettes s'affichent ensuite comme sous-catégories de la catégorie *People (Gens)* :

    a. Créez une nouvelle étiquette intitulée `Amis`.

    b. Créez une nouvelle étiquette intitulée `Famille`.

3. Associez maintenant ces étiquettes aux images ou aux groupes d'images sélectionnés. Cliquez avec le bouton droit de la souris sur une image, choisissez *Attach*

Tag (Attacher l'étiquette), puis sélectionnez l'étiquette appropriée pour cette image. Pour associer une étiquette à un groupe d'images, cliquez sur la première image et, tout en maintenant la touche Shift enfoncée, sélectionnez les autres images de votre choix. Shift Cliquez avec le bouton droit de la souris pour afficher le menu de l'étiquette et sélectionnez la catégorie correspondante.

Une fois les images classées en catégories, vous pouvez parcourir votre collection en fonction des étiquettes. Il suffit de cocher *People (Gens)* → *Famille* pour limiter la collection affichée aux images portant l'étiquette `Famille`. Grâce au menu *Find (Rechercher)* → *Find by Tag (Rechercher par étiquette)*, vous pouvez également faire des recherches par étiquettes dans votre collection. Les résultats de votre recherche s'affichent dans la fenêtre de présentation des miniatures.

Que vous supprimiez des étiquettes d'images individuelles ou de groupes d'images, ou que vous associez des étiquettes à ces images, le principe est le même. Les fonctions d'édition des étiquettes sont également accessibles via le menu *Tags (Étiquettes)* de la barre de menus supérieure.

15.5.4 Recherches

Comme indiqué à la Section 15.5.3, « Gestion des onglets » (p. 233), les étiquettes permettent de rechercher certaines images. Une autre méthode, qui est une exclusivité f-spot, consiste à utiliser la *ligne de temps* sous la barre d'outils. Faites glisser le petit cadre le long de cette ligne de temps pour restreindre l'affichage des images dans la présentation des miniatures à celles prises dans le cadre temporel sélectionné. f-spot démarre avec une ligne de temps par défaut choisie avec soin, mais vous pouvez la modifier en déplaçant les curseurs vers les extrémités gauche et droite de cette ligne.

15.5.5 Exportation des collections d'images

f-spot offre toute une gamme de fonctions d'exportation pour vos collections via le menu *File (Fichier)* → *Export (Exporter)*. Les options les plus fréquemment utilisées de ce menu sont probablement *Export to Web Gallery (Exporter vers la galerie Web)* et *Export to CD (Exporter vers un CD)*.

Pour exporter une sélection d'images dans une galerie Web, procédez comme suit :

1. Sélectionnez les images à exporter.

2 Cliquez sur *File (Fichier) → Export (Exporter) → Export to Web Gallery (Exporter vers la galerie Web)*, puis sélectionnez la galerie vers laquelle exporter vos images ou ajoutez-en une nouvelle. f-spot établit une connexion avec l'emplacement Web entré pour votre galerie Web. Sélectionnez l'album vers lequel exporter les images, et indiquez si ces dernières doivent être mises à l'échelle automatiquement et s'il faut exporter leurs titres et commentaires.

Figure 15.8 *Exportation d'images dans une galerie Web*



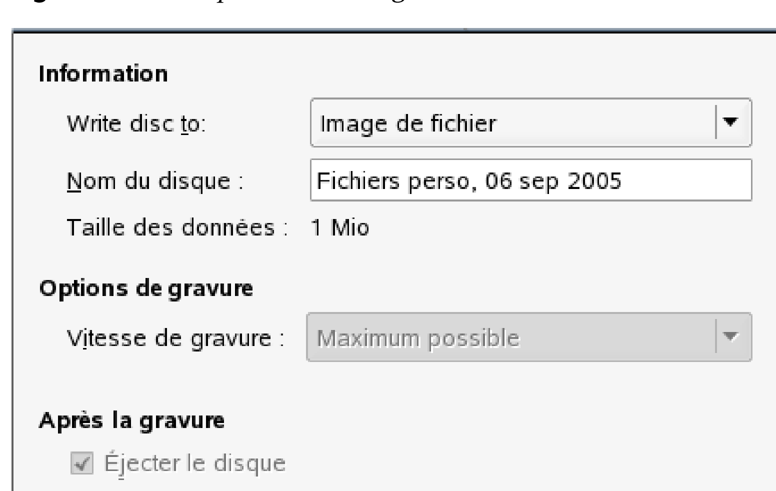
Pour exporter une sélection d'images sur un CD, procédez comme suit :

1 Sélectionnez les images à exporter.

2 Cliquez sur *File (Fichier) → Export (Exporter) → Export to CD (Exporter vers un CD)*, puis sur *OK*.

f-spot copie les fichiers et ouvre la boîte de dialogue d'écriture sur un CD. Assignez un nom à votre disque d'image et déterminez la vitesse d'écriture. Cliquez sur *Write (Écrire)* pour lancer le processus d'écriture sur le CD.

Figure 15.9 *Exportation d'images sur un CD*



15.5.6 Traitement de base des images dans f-spot

f-spot propose plusieurs fonctionnalités très simples d'édition d'images. Entrez en mode d'édition de f-spot en cliquant sur l'icône *Edit Image (Modifier l'image)* de la barre d'outils ou en double-cliquant sur l'image à modifier. Passez d'une image à l'autre à l'aide des flèches en bas à droite. Choisissez parmi les fonctions d'édition suivantes :

Sharpen (Préciser)
: Accédez à cette fonction via le menu *Edit (Édition)* → *Sharpen (Préciser)*. Réglez les valeurs des paramètres *Amount (Quantité)*, *Radius (Rayon)* et *Threshold (Seuil)* en fonction de vos besoins, puis cliquez sur *OK*.

Crop Image (Rogner l'image)
: Pour rogner l'image en fonction de la sélection effectuée, choisissez un rapport hauteur/largeur fixe ou l'option *No Constraint (Pas de contrainte)* dans le menu déroulant en bas à gauche, sélectionnez la zone à rogner, puis cliquez sur la paire de ciseaux à côté du menu des rapports de rognage.

Red Eye Reduction (Réduction de l'effet yeux rouges)
Sur un portrait, sélectionnez la zone du visage avec les yeux et cliquez sur l'icône représentant un œil rouge.

Adjust Color (Régler la couleur)
Affichez l'histogramme utilisé lors de la création du cliché et corrigez l'exposition et la température des couleurs, si nécessaire.

ASTUCE: Traitement avancé des images

Vous pouvez éditer des images de façon professionnelle dans GIMP. Pour plus d'informations sur GIMP, reportez-vous au Chapitre 17, *Manipulation des graphiques au moyen de GIMP* (p. 247).

15.6 Pour plus d'informations

Pour plus d'informations concernant l'utilisation d'appareils photo numériques avec Linux, reportezvous aux sites Web suivants.

- `http://digikam.sourceforge.net/` : informations relatives à Digikam
- `http://www.gphoto.org` : informations relatives à gPhoto2
- `http://www.gphoto.org/proj/libgphoto2/support.php` : liste complète des appareils photo pris en charge
- `http://www.thekompany.com/projects/gphoto/` : informations relatives à Kamera, une interface cliente de KDE pour gPhoto2

Kooka — Application de numérisation

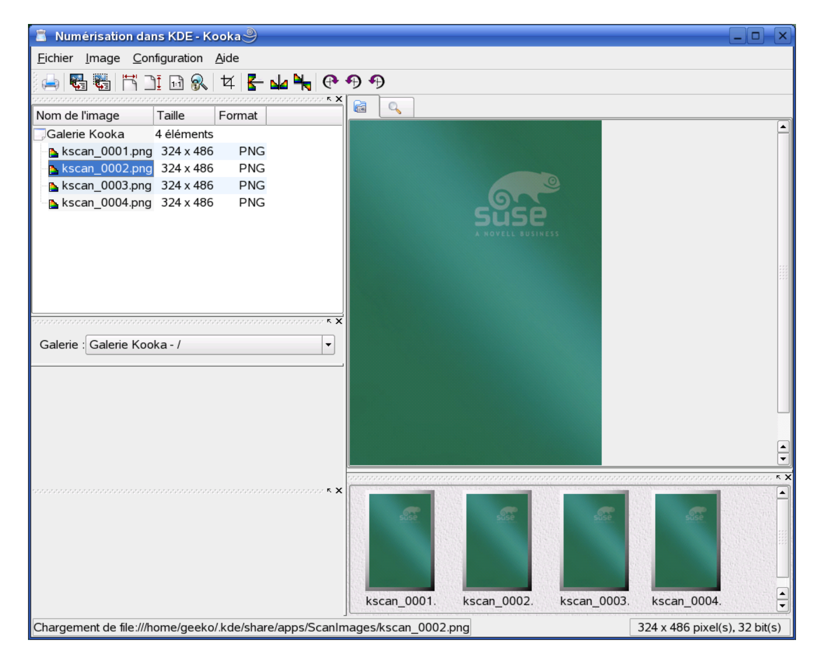
16

Kooka est une application de numérisation KDE. Ce chapitre présente l'interface utilisateur et le fonctionnement de l'application. Outre la création de fichiers image à partir d'un support imprimé (photos ou magazines, par exemple), Kooka offre des fonctions de reconnaissance de caractères. Il permet donc de convertir du texte en un fichier texte qui peut être modifié.

Start Kooka (Démarrez Kooka) à partir du menu principal ou en tapant la commande `kooka`. Au démarrage, Kooka ouvre une fenêtre qui comporte trois cadres, une barre de menus en haut à gauche et une barre d'outils tout juste en dessous. Toutes les fenêtres peuvent être réorganisées et rajustées à l'aide de la souris. Il est également possible de détacher les cadres de la fenêtre de Kooka afin de les placer à l'endroit voulu sur le bureau. Pour déplacer un cadre, cliquez sur la fine double ligne tout juste au-dessus et glissez-le à l'endroit voulu. Chaque cadre, à l'exception de la fenêtre principale, peut être placé à l'intérieur d'un autre et aligné à gauche, à droite, en haut, en bas ou au milieu. Les fenêtres centrées ont la même taille. Elles sont empilées et peuvent être amenées à l'avant-plan au moyen d'onglets.

Par défaut, les cadres *Afficheur d'images* et *Aperçu de numérisation* partagent la même fenêtre. Des onglets permettent de passer de l'un à l'autre. Le cadre de gauche contient la galerie. La galerie est un petit explorateur de fichiers permettant d'accéder aux images numérisées. Le cadre en bas à droite est partagé par la ROC (reconnaissance optique des caractères) et les vignettes, qui peuvent être chargées dans l'afficheur d'images par un simple clic de souris. (voir Figure 16.1, « La fenêtre principale de Kooka » (p. 240)).

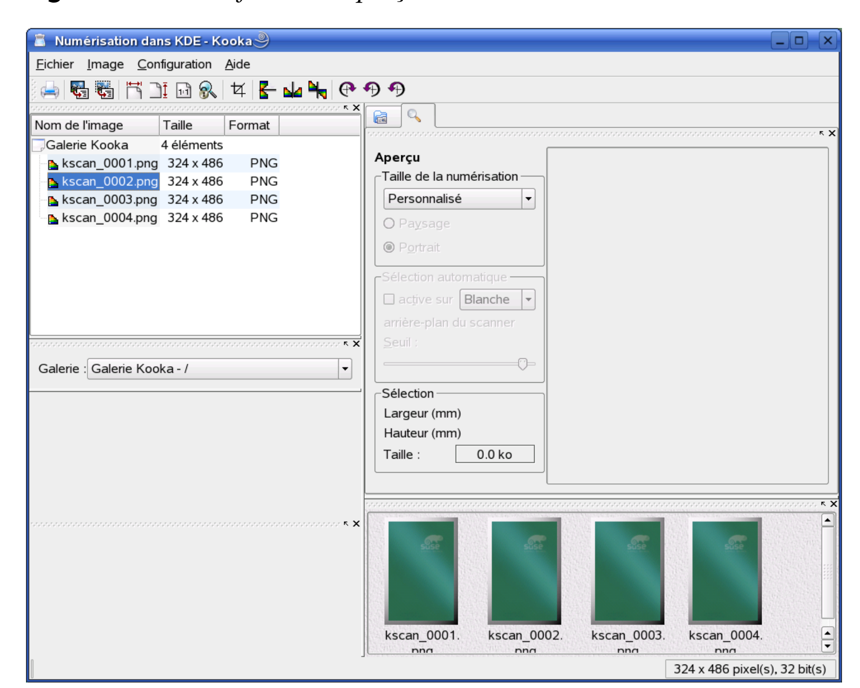
Figure 16.1 *La fenêtre principale de Kooka*



16.1 L'aperçu

Lorsque l'objet à numériser est plus petit que la zone totale de numérisation, il faut toujours en créer un aperçu. Définissez quelques paramètres à gauche de la fenêtre d'aperçu. Fixez la taille de numérisation avec l'option *Personnalisée* ou choisissez un des formats standard. (voir Figure 16.2, « La fenêtre d'aperçu de Kooka » (p. 241)). Le paramètre *Personnalisée* offre le plus de flexibilité parce qu'il permet de délimiter la zone souhaitée à l'aide de la souris. Après avoir défini les paramètres, générez l'aperçu de l'image à numériser en cliquant sur *Aperçu* dans *Paramètres de numérisation*.

Figure 16.2 *La fenêtre d'aperçu de Kooka*

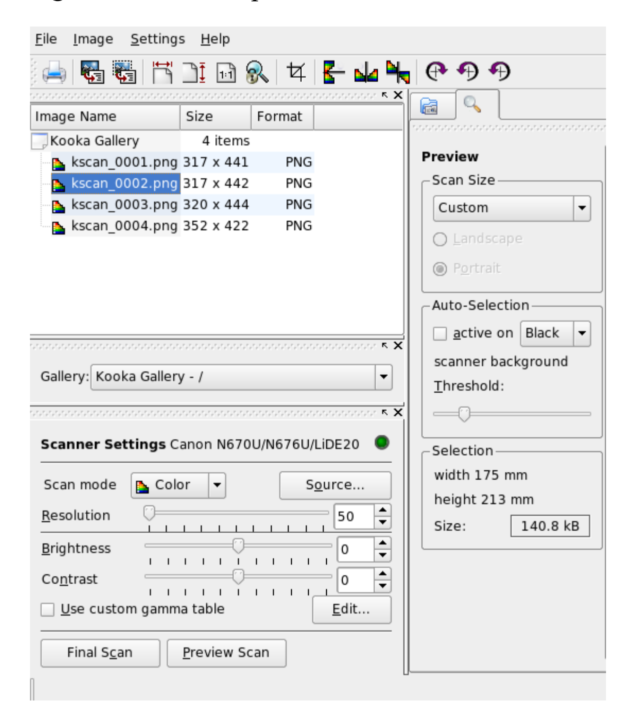


16.2 La numérisation finale

Si vous avez sélectionné *Personnalisée* comme taille de numérisation, utilisez la souris pour tracer le rectangle à numériser. La zone sélectionnée est délimitée par une bordure pointillée.

Choisissez une numérisation en couleur ou en noir et blanc et réglez la résolution au moyen de la glissière. (voir Figure 16.3, « Les paramètres de numérisation de Kooka » (p. 242)). Plus la résolution est élevée, plus l'image numérisée est de bonne qualité. Toutefois, la taille du fichier final est également plus importante et la numérisation peut durer très longtemps. Activez la *Table gamma personnalisée* et cliquez sur *Modifier* afin de pouvoir régler les paramètres de luminosité, de contraste et le gamma.

Figure 16.3 *Les paramètres de numérisation de Kooka*



Dès que tous les paramètres ont été définis, cliquez sur *Numérisation finale* pour numériser l'image. L'image numérisée apparaît ensuite dans l'afficheur d'images et sous forme de vignette. À l'invite, sélectionnez le format de l'image enregistrée. Pour enregistrer toutes les images au même format, cochez la case prévue à cet effet. Cliquez sur *OK* pour confirmer.

16.3 Les menus

Les fonctions de la barre d'outils sont en partie accessibles à partir des menus *Fichier* et *Image*. Modifiez les préférences de Kooka dans *Settings* (Paramètres).

Fichier

Utilisez ce menu pour lancer l'assistant d'impression KPrinter, pour créer un dossier pour vos images, et pour enregistrer, supprimer et fermer des fichiers. Ce menu

vous permet également d'enregistrer le résultat de la ROC d'un texte numérisé. Enfin, c'est à partir de ce menu que vous pouvez fermer Kooka.

Image

Le menu *Image* permet de lancer une application graphique pour le traitement ou la reconnaissance optique des caractères d'une image. Le texte reconnu suite à une ROC s'affiche dans un cadre à part. Plusieurs outils sont mis à votre disposition pour réduire, agrandir, retourner ou faire pivoter vos images. Ces fonctions sont également accessibles à partir de la barre d'outils. Le menu *Create From Selection* (Créer à partir de la sélection) permet d'enregistrer une partie d'une image préalablement délimitée au moyen de la souris.

Paramètres

L'option *Settings* (Paramètres) vous permet de régler l'apparence et le style de Kooka. Vous pouvez notamment activer ou désactiver la barre d'outils et la barre d'état, ou encore définir les raccourcis clavier pour les entrées de menus. L'option *Configurer les barres d'outils* regroupe une liste de toutes les fonctions auxquelles vous pouvez accéder à partir de la barre d'outils. L'option *Configure Kooka* (Configurer Kooka) ouvre une boîte de dialogue de configuration dans laquelle vous pouvez modifier l'apparence et le style de Kooka. Normalement, les paramètres par défaut sont suffisants. Dans *Afficher les outils*, activez et désactivez l'affichage en vignettes, l'aperçu, la galerie, les paramètres de numérisation, et la fenêtre de résultat de la ROC.

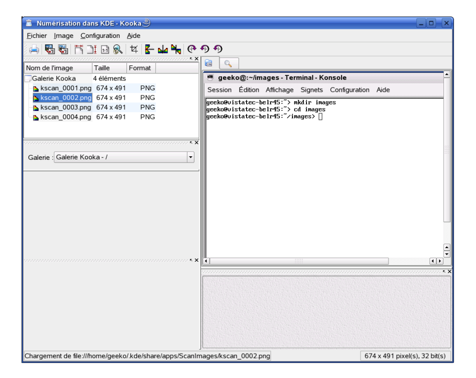
Aide

Le menu *Help* (Aide) permet d'accéder au manuel d'aide en ligne de Kooka. Utilisez-le également pour accéder à un canal de feed-back qui vous permet de signaler un problème ou de faire part d'une suggestion. Il fournit également des informations sur la version, les auteurs et la licence de Kooka et de KDE.

16.4 La galerie

La galerie présente le contenu du dossier par défaut dans lequel Kooka stocke toutes ses images. La Figure 16.4, « La galerie de Kooka » (p. 244) vous en montre un exemple. Pour enregistrer une image dans votre dossier personnel, cliquez sur sa vignette pour la sélectionner, puis sélectionnez *Fichier* → *Enregistrer l'image*. Ensuite, tapez le chemin d'accès de votre répertoire personnel et donnez au fichier un nom descriptif.

Figure 16.4 *La galerie de Kooka*

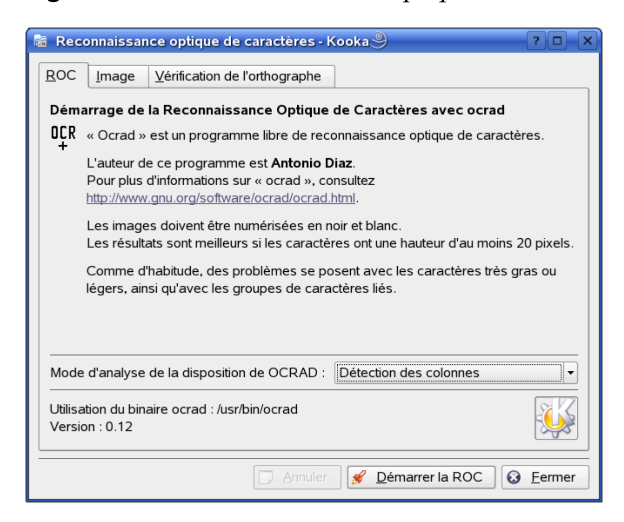


Pour ajouter des images à la galerie, importez-les depuis Konqueror au moyen d'un simple glisser-déplacer. Démarrez Konqueror, accédez au répertoire qui contient les images à ajouter à la galerie, puis faites glisser les images à l'aide de la souris vers un dossier de la galerie Kooka.

16.5 Reconnaissance optique des caractères

Si le module de reconnaissance des caractères est installé, vous pouvez numériser les documents en mode *lineart*, les enregistrer dans le format proposé, puis lancer la reconnaissance à partir du menu *Image*. Reconnaissez la totalité du document ou une zone préalablement délimitée. Une boîte de dialogue de configuration permet d'indiquer au module si le texte original est imprimé, manuscrit ou normalisé. Définissez également la langue afin que le module puisse traiter le document correctement. (voir Figure 16.5, « Reconnaissance optique de caractères (ROC) avec Kooka » (p. 245)).

Figure 16.5 Reconnaissance optique de caractères (ROC) avec Kooka



Activez la fenêtre *Résultat de la ROC* et vérifiez le texte, qui aura peut-être besoin d'une relecture. Pour ce faire, enregistrez le texte en sélectionnant *Fichier → Enregistrer le résultat de la ROC*. Le texte peut ensuite être traité dans OpenOffice.org ou KWrite.

Manipulation des graphiques au moyen de GIMP 17

GIMP (GNU Image Manipulation Program - *logiciel de manipulation d'images du GNU*) est un programme qui permet de créer et de modifier les graphiques en pixels. Pour la plupart, ses fonctions sont comparables à celles d'Adobe Photoshop et d'autres programmes commerciaux. Vous pouvez l'utiliser pour redimensionner et retoucher des photos, créer des graphiques pour des pages web, créer des pochettes personnalisées pour vos CD, ou presque tout autre projet graphique. Il répond aux besoins à la fois des amateurs et des professionnels.

Comme de nombreux autres programmes Linux, GIMP est le fruit d'une coopération entre des développeurs du monde entier qui ont accepté de consacrer leur temps et leurs lignes de code à ce projet. Le programme est en évolution constante, c'est pourquoi la version incluse dans votre SUSE LINUX peut différer légèrement de la version proposée ici. La disposition des différentes fenêtres et sections de fenêtres en particulier est susceptible de changer.

GIMP est un programme extrêmement complexe. Seul un petit nombre de fonctions, d'outils et d'éléments de menu sont présentés dans ce chapitre. Pour savoir où trouver d'autres informations sur le programme, consultez la Section 17.6, « Pour plus d'informations » (p. 254).

17.1 Formats de graphiques

Il existe deux formats de graphiques principaux : en pixels et vectoriels. GIMP fonctionne uniquement avec des graphiques en pixels, qui constituent le format standard pour les photos et les images numérisées. Les graphiques en pixels se composent de

petits blocs de couleur qui créent ensemble l'image complète. C'est pourquoi les fichiers peuvent très vite atteindre une taille importante. Il est impossible d'augmenter la taille d'une image en pixels sans perdre de sa qualité.

À la différence des graphiques en pixels, les graphiques vectoriels ne stockent pas d'informations pour chaque pixel. En revanche, ils stockent des informations concernant la manière dont sont regroupés les points, les lignes ou les zones de l'image. Les images vectorielles peuvent être redimensionnées très facilement. Par exemple, l'application de dessin d'OpenOffice.org utilise ce format.

17.2 Démarrage de GIMP

Démarrez GIMP à partir du menu principal. Vous pouvez également entrer `gimp &` dans une ligne de commande.

17.2.1 Configuration initiale

Lorsque vous démarrez GIMP pour la première fois, un assistant de configuration apparaît pour préparer la configuration. Les paramètres par défaut conviennent à la plupart des utilisations. Appuyez donc sur *Continuer* dans chaque boîte de dialogue à moins que vous ne connaissiez les paramètres et préfériez une autre configuration.

17.2.2 Les fenêtres par défaut

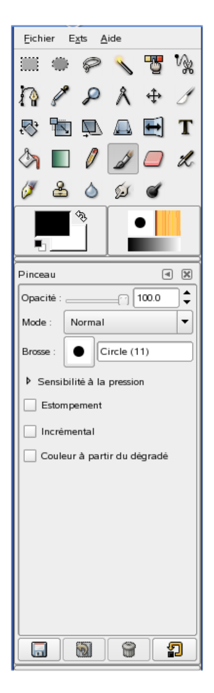
Trois fenêtres apparaissent par défaut. Elles peuvent figurer à l'écran ou être fermées, à l'exception de la boîte à outils, si elles ne sont plus nécessaires. La fermeture de la boîte à outils entraîne la fermeture de l'application. Dans la configuration par défaut, GIMP enregistre la disposition des fenêtres lorsque vous quittez l'application. Les boîtes de dialogue restées ouvertes réapparaîtront la prochaine fois que vous lancerez le programme.

La boîte à outils

La fenêtre principale de GIMP, illustrée par la Figure 17.1, « La fenêtre principale » (p. 249), contient les principaux contrôles de l'application. La fermeture de cette fenêtre entraîne la fermeture de l'application. Tout en haut, la barre de menus donne accès aux

fonctions et extensions du fichier, ainsi qu'à la rubrique d'aide. En dessous se trouvent les icônes des différents outils. Pointez la souris sur une icône pour afficher les informations la concernant.

Figure 17.1 *La fenêtre principale*



Les couleurs actuelles de premier plan et d'arrière-plan apparaissent dans deux zones superposées. Par défaut, la couleur de premier plan est noire et la couleur d'arrière-plan est blanche. Cliquez sur la zone pour ouvrir une boîte de dialogue de sélection des couleurs. Permutez les couleurs de premier plan et d'arrière-plan à l'aide du symbole de flèche coudée dans le coin supérieur droit des zones. Utilisez le symbole noir et blanc dans le coin inférieur gauche pour réinitialiser les couleurs par défaut.

À droite sont affichés le pinceau, le motif et le dégradé actuels. Cliquez sur l'élément affiché pour accéder à la boîte de dialogue de sélection. La partie inférieure de la fenêtre permet la configuration des diverses options pour l'outil actuel.

Calques, Canaux, Chemins, Annuler

Dans la première section, utilisez la zone de liste déroulante pour sélectionner l'image à laquelle se réfère l'onglet. En cliquant sur *Auto*, vérifiez si l'image active est sélectionnée automatiquement. L'option *Auto* est activée par défaut.

Calques affiche les différents calques des images actuelles et permet de les manipuler. *Canaux* affiche les canaux de couleur de l'image et permet de les manipuler.

Les chemins offrent une méthode avancée pour sélectionner les parties d'une image. Ils peuvent servir également au dessin. *Chemins* affiche les chemins disponibles pour une image et donne accès à leurs fonctions. *Annuler* affiche un historique restreint des modifications apportées à l'image actuelle.

La partie inférieure de la fenêtre contient trois onglets. Ceux-ci vous permettent de sélectionner le pinceau, le dégradé et le motif actuels.

17.3 Mise en route de GIMP

Bien que GIMP puisse être un peu complexe pour les nouveaux utilisateurs, la plupart d'entre eux le trouvent très vite facile à utiliser, une fois qu'ils ont acquis quelques notions de base. Les fonctions de base cruciales sont la création, l'ouverture et l'enregistrement d'images.

17.3.1 Création d'une nouvelle image

Pour créer une image, sélectionnez *File (Fichier)* → *New (Nouveau)* ou appuyez sur Ctrl + N. Cela vous permet d'ouvrir une boîte de dialogue dans laquelle vous pouvez paramétrer la nouvelle image. Si vous le souhaitez, utilisez l'option *Template* (Modèle) pour sélectionner le modèle qui servira de base à la nouvelle image. GIMP offre plusieurs modèles, qui vont de la feuille de papier A4 à la pochette de CD. Pour créer un modèle personnalisé, sélectionnez *Fichier* → *Dialogs* (Dialogues) *Modèles...* et utilisez les commandes proposées dans la fenêtre ouverte.

Dans la section *Taille de l'image*, définissez la taille de l'image à créer en pixels ou dans une autre unité. Cliquez sur l'unité pour en sélectionner une autre dans la liste proposée. Le rapport entre les pixels et une autre unité est défini sous *Resolution*

(Résolution), accessible lorsque la section *Advanced Options* (Options avancées) est ouverte. Une résolution de 72 pixels par pouce correspond à l'écran d'affichage. Cela suffit pour les graphiques des pages web. Une résolution supérieure est toutefois conseillée pour les images à imprimer. Pour la plupart des imprimantes, une résolution de 300 pixels par pouce donne une qualité acceptable.

Sous *Colorspace* (Espace de couleurs), déterminez si l'image doit apparaître en couleurs (*RGB*) ou en *niveaux de gris*. Sélectionnez l'option *Type de remplissage* pour la nouvelle image. Les options *Foreground Color* (Couleur de premier plan) et *Background Color* (Couleur d'arrière-plan) utilisent les couleurs sélectionnées dans la boîte à outils. L'option *Blanc* utilise un arrière-plan blanc dans l'image. L'option *Transparent* crée une image transparente. La *transparence* est représentée par un motif de damier gris. Entrez un commentaire pour la nouvelle image sous *Comment* (Commentaire).

Lorsque les paramètres répondent à vos besoins, appuyez sur *OK*. Pour restaurer les paramètres par défaut, appuyez sur *Réinitialiser*. Si vous appuyez sur *Annuler*, vous abandonnez la création d'une nouvelle image.

17.3.2 Ouverture d'une image existante

Pour ouvrir une image existante, sélectionnez *File (Fichier) → Open (Ouvrir)* ou appuyez sur Ctrl + O. Dans la boîte de dialogue qui apparaît, sélectionnez le fichier souhaité. Cliquez sur *OK* pour ouvrir l'image sélectionnée. Cliquez sur *Annuler* si vous ne souhaitez ouvrir aucune image.

17.3.3 La fenêtre d'image

L'image nouvelle ou ouverte apparaît dans sa propre fenêtre. La barre de menus en haut de la fenêtre permet d'accéder aux fonctions de l'image. Vous pouvez également accéder au menu en cliquant avec le bouton droit sur l'image ou en cliquant sur le petit bouton en forme de flèche situé dans le coin gauche des règles.

Fichier offre les options standard du fichier, telles que *Enregistrer* et *Imprimer*. *Fermer* ferme l'image actuelle. *Quitter* ferme toute l'application.

Les éléments du menu *View* (Affichage) vous permettent de contrôler l'affichage et la fenêtre de l'image. *Nouvel affichage* ouvre une seconde fenêtre d'affichage de l'image actuelle. Les modifications apportées à un affichage se reflètent dans tous les autres

affichages de cette image. D'autres affichages permettent d'agrandir une partie de l'image pour la manipulation, tandis que l'image complète apparaît dans un autre affichage. Réglez le coefficient de grossissement de la fenêtre actuelle à l'aide du *zoom*. Lorsque l'option *Shrink Wrap* (Ajuster la fenêtre à l'image) est sélectionnée, la fenêtre d'image est redimensionnée pour s'adaptée exactement à l'affichage de l'image actuelle.

17.4 Enregister des images

Aucune fonction de gestion d'images n'est aussi importante que *File (Fichier) → Save (Enregistrer)*. Il est donc préférable d'enregistrer trop souvent plutôt que trop rarement. Utilisez *File (Fichier) → Save as (Enregistrer sous)* pour enregistrer l'image sous un nouveau nom. Il est judicieux d'enregistrer les étapes de l'image sous différents noms ou de faire des sauvegardes dans un autre répertoire afin de pouvoir restaurer facilement un état antérieur.

Lorsque vous enregistrez un fichier pour la première fois ou que vous utilisez *Save as (Enregistrer sous)*, une boîte de dialogue s'ouvre, et permet de spécifier le nom et le type du fichier. Entrez le nom du fichier dans le champ situé en haut. Sous *Save in folder* (Enregistrer dans le dossier), sélectionnez le répertoire où enregistrer le fichier, dans la liste de ceux qui sont le plus souvent utilisés. Pour utiliser un autre répertoire ou en créer un, ouvrez *Browse for other folders* (Parcourir pour trouver d'autres dossiers). Il est recommandé de laisser *Determine File Type* (Déterminer le type du fichier) défini sur *By Extension* (Selon l'extension). Avec ce paramètre, GIMP détermine le type de fichier, sur la base de l'extension du nom de ce fichier. Les types de fichiers suivants sont souvent utiles :

XCF
: Il s'agit du format natif de l'application. Il enregistre toutes les informations sur les calques et les chemins en même temps que l'image. Même si vous avez besoin d'une image dans un autre format, il est généralement recommandé d'enregistrer une copie dans le format XCF pour simplifier les futures modifications.

PAT
: Il s'agit du format utilisé pour les motifs GIMP. L'enregistrement d'une image dans ce format permet d'utiliser l'image comme motif de remplissage dans GIMP.

JPG
: JPG ou JPEG est un format commun aux photos et graphiques de pages web sans transparence. Sa méthode de compression permet de réduire les tailles des fichiers,

mais entraîne une perte d'informations. L'option de prévisualisation peut s'avérer utile pour régler le niveau de compression. Des niveaux de 85 % à 75 % ont souvent pour résultat une qualité d'image acceptable à une compression raisonnable. L'enregistrement d'une sauvegarde dans le format sans perte, tel que XCF, est également recommandé. Si vous modifiez une image, enregistrez seulement l'image finie dans le format JPG. Le fait de charger un JPG à plusieurs reprises et de l'enregistrer peut rapidement donner une qualité d'image médiocre.

GIF

Même s'il était très populaire par le passé pour les graphiques avec transparence, aujourd'hui le format GIF est utilisé plus rarement en raison des problèmes de licences. Le format GIF est utilisé également pour les images animées. Il permet seulement d'enregistrer des images *indexées*. Souvent, la taille du fichier peut être relativement petite si quelques couleurs seulement sont utilisées.

PNG

Grâce à la prise en charge de la transparence, à la compression sans perte, à la libre disponibilité et à une meilleure gestion du navigateur, le format PNG remplace le format GIF en tant que format préféré pour les graphiques Web avec transparence. Le format PNG présente un avantage supplémentaire, celui d'offrir une transparence partielle, ce que ne permet pas le format GIF. Cela permet de réaliser des transitions plus en douceur depuis les zones de couleur vers les zones transparentes (*anticrénelage*).

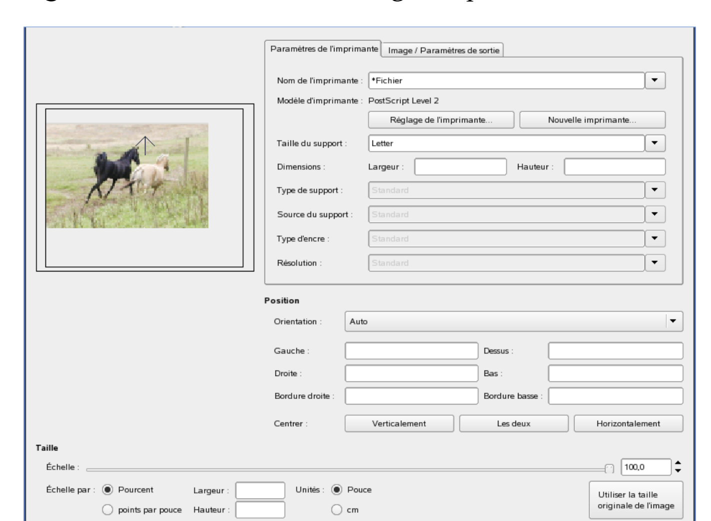
Pour enregistrer l'image dans le format choisi, cliquez sur *Enregistrer*. Pour abandonner, appuyez sur *Annuler*. Si l'image présente des caractéristiques qui ne peuvent pas être enregistrées dans le format choisi, une boîte de dialogue apparaît avec des choix pour résoudre la situation. Si elle est disponible, l'option *Exporter* donne normalement les résultats souhaités. Une fenêtre s'ouvre alors avec les options du format. Des valeurs par défaut raisonnables sont fournies.

17.5 Impression des images

Pour imprimer une image, sélectionnez *File (Fichier)* → *Print (Imprimer)* dans le menu de l'image. Si votre imprimante est configurée dans SUSE, elle doit apparaître dans la liste. Dans certains cas, il peut s'avérer nécessaire de sélectionner un pilote approprié grâce à l'option *Configurer l'imprimante*. Sélectionnez la taille de papier appropriée dans *Media Size (Taille de support)* et le type dans *Media Type (Type de support)*.

D'autres paramètres sont disponibles dans l'onglet *Image / Paramétrage pour l'impression*.

Figure 17.2 *La boîte de dialogue Imprimer*



Ajustez la taille de l'image dans la partie inférieure de la fenêtre. Cliquez sur *Use Original Image Size* (Utiliser la taille originale de l'image) pour reprendre ces paramètres à partir de l'image elle-même. Cela est recommandé si vous avez défini une taille d'impression et une résolution appropriées. Ajustez la position de l'image sur la page à l'aide des champs figurant sous *Position* ou en faisant glisser l'image dans *Prévisualiser*.

Si les paramètres vous conviennent, cliquez sur *Imprimer*. Si vous souhaitez enregistrer les paramètres pour une utilisation future, cliquez plutôt sur *Print and Save Settings* (Imprimer et enregistrer les réglages). *Annuler* interrompt l'impression.

17.6 Pour plus d'informations

Les ressources suivantes peuvent s'avérer utiles à l'utilisateur GIMP. Malheureusement, de nombreuses ressources s'appliquent à des versions antérieures.

- *Aide* donne accès au système d'aide interne. Cette documentation est également disponible aux formats HTML et PDF, à l'adresse `http://docs.gimp.org`.

- Le groupe d'utilisateurs GIMP propose un site Web instructif et intéressant, à l'adresse `http://gug.sunsite.dk`.

- `http://www.gimp.org` est la page d'accueil officielle de GIMP.

- *Grokking the GIMP* est un excellent livre de Carey Bunks qui s'appuie sur une version antérieure de GIMP. Bien que certains aspects du programme aient changé, il constitue toujours un excellent guide pour la manipulation des images. Une version en ligne est disponible à l'adresse `http://gimp-savvy.com/BOOK/`.

- `http://gimp-print.sourceforge.net` est la page Web du plug-in d'impression GIMP. Le manuel d'utilisateur disponible sur le site fournit des informations détaillées sur la configuration et l'utilisation du programme.



Mobilité

Informatique mobile avec Linux 18

Ce chapitre présente différents aspects de l'utilisation de Linux dans le cadre de l'informatique mobile. Vous trouverez une introduction rapide des différents champs d'utilisation, suivie d'une description des fonctions essentielles du matériel utilisé. Vous trouverez également exposées des solutions logicielles pour répondre à des exigences spéciales et des options pour obtenir des performances maximales, ainsi que des méthodes pour réduire la consommation d'énergie. Une présentation des sources d'informations les plus importantes sur ce sujet viendra clore ce chapitre.

La plupart des gens associent l'informatique mobile aux ordinateurs portables, aux assistants personnels (PDA) et aux téléphones cellulaires, ainsi qu'à l'échange de données entre ces dispositifs. Ce chapitre élargit cet horizon aux composants matériels mobiles (disques durs externes, lecteurs Flash, appareils photo numériques, etc.) que vous pouvez connecter à des ordinateurs portables ou à des systèmes de bureau.

18.1 Ordinateurs portables

Le matériel des ordinateurs portables est différent de celui d'un système de bureau classique. En effet, l'interchangeabilité, l'espace occupé et la consommation d'énergie sont des critères qui ont leur importance. Les fabricants de matériel mobile ont développé la norme PCMCIA (Personal Computer Memory Card International Association). Cette norme concerne les cartes mémoire, les cartes d'interface réseau, les cartes RNIS et modem, et les disques durs externes. Pour obtenir des informations sur la mise en œuvre sous Linux de la prise en charge de ce type de matériel, sur les besoins dont il faut tenir compte au cours de la configuration, sur les logiciels disponibles pour

le contrôle de la norme PCMCIA et sur le dépannage des problèmes éventuels, reportez-vous au Chapitre 19, *PCMCIA* (p. 271).

18.1.1 Économie d'énergie

Le processus de fabrication des ordinateurs portables intégrant l'utilisation de composants système optimisés en matière d'alimentation, ces ordinateurs sont parfaitement adaptés pour être utilisés sans être relié au réseau électrique. La contribution de ces composants en matière d'économie d'énergie est au moins aussi importante que celle du système d'exploitation. SUSE Linux prend en charge différentes méthodes qui ont une influence sur la consommation d'énergie d'un ordinateur portable et qui ont des effets variables sur le temps de fonctionnement de ce dernier sur batterie. Dans la liste suivante, ces méthodes sont classées par ordre décroissant, en fonction de l'économie d'énergie représentée :

- Limitation de la vitesse de l'unité centrale
- Désactivation de l'éclairage de l'écran pendant les pauses
- Réglage manuel de l'éclairage de l'écran
- Déconnexion des accessoires enfichables à chaud non utilisés (CD-ROM USB, souris externe, cartes PCMCIA, etc.)
- Ralentissement du disque dur en phase d'inactivité

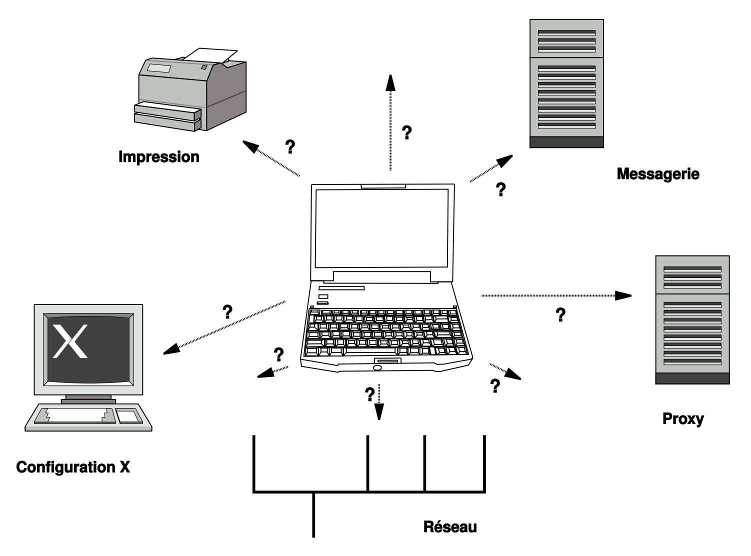
Pour plus d'informations sur la gestion de l'alimentation sous SUSE Linux et sur l'exploitation du module de gestion de l'alimentation YaST, reportez-vous au Chapitre 21, *Gestion de l'alimentation* (p. 285).

18.1.2 Intégration dans des environnements d'exploitation en perpétuelle évolution

Lorsque vous l'utilisez dans le cadre de l'informatique mobile, votre système a besoin de s'adapter en permanence aux évolutions des environnements d'exploitation. De

nombreux services dépendent de l'environnement : il faut alors reconfigurer les clients sous-jacents. SUSE Linux se charge de ces tâches pour vous.

Figure 18.1 *Intégration d'un ordinateur portable à un réseau*



Les services suivants sont affectés lorsqu'un ordinateur portable fait sans cesse la navette entre un petit réseau privé et un réseau professionnel :

Configuration réseau
Cela comprend l'assignation d'adresses IP, la résolution des noms, la connectivité Internet et la connectivité à d'autres réseaux.

Impression
La présence d'une base de données actualisée des imprimantes disponibles et d'un serveur d'impression disponible est requise, en fonction du réseau.

Messagerie électronique et applications proxy
Comme pour l'impression, la liste des serveurs correspondants doit être actualisée.

Configuration de X
Si votre ordinateur portable est temporairement connecté à un projecteur infrarouge ou à un moniteur externe, les différentes configurations d'affichage doivent être disponibles.

SUSE Linux offre deux méthodes pour intégrer un ordinateur portable à des environnements d'exploitation existants. Vous pouvez les combiner.

SCPM

La méthode SCPM (System Configuration Profile Management - gestion des profils de configuration système) permet de stocker des états de configuration arbitraires d'un système dans une sorte de « cliché » appelé *profil*. Vous pouvez créer des profils pour différentes situations. Ils sont pratiques lorsqu'un système est exécuté dans des environnements en perpétuelle évolution (réseau privé ou professionnel). Il est toujours possible de basculer d'un profil à l'autre. Pour plus d'informations sur la méthode SCPM, reportez-vous au Chapitre 20, *Gestion du profil de configuration du système (SCPM, System Configuration Profile Management)* (p. 273). Dans KDE, l'applet du Kicker du sélectionneur de profils permet de basculer entre les différents profils. L'application a besoin du mot de passe root pour pouvoir effectuer ce basculement.

SLP

Le protocole SLP (Service Location Protocol) simplifie la connexion d'un ordinateur portable à un réseau existant. Sans le protocole SLP, l'administrateur d'un ordinateur portable a généralement besoin d'informations détaillées sur les services disponibles sur un réseau. Le protocole SLP diffuse la disponibilité des services d'un certain type à tous les clients d'un réseau local. Les applications prenant en charge le protocole SLP peuvent traiter les informations distribuées par le protocole SLP et être configurées automatiquement. Vous pouvez même utiliser le protocole SLP pour installer un système, sans avoir à rechercher une source d'installation appropriée. Pour plus d'informations sur le protocole SLP, reportez-vous au Chapitre 39, *Services SLP sur le réseau* (p. 651).

Le point fort de la méthode SCPM réside dans l'activation et l'entretien de conditions système reproductibles. Le protocole SLP facilite considérablement la configuration d'un ordinateur appartenant à un réseau en automatisant la majeure partie de cette opération.

18.1.3 Options logicielles

Dans le cadre d'une utilisation mobile, il existe plusieurs catégories de tâches spéciales couvertes par des logiciels dédiés : la surveillance du système (notamment la charge des batteries), la synchronisation des données et la communication sans fil entre les

périphériques et Internet. Les sections suivantes traitent des principales applications que SUSE Linux propose pour chaque tâche.

Surveillance du système

SUSE Linux propose deux outils de surveillance du système KDE. L'affichage de l'état exact de la batterie rechargeable de l'ordinateur portable est géré par l'applet KPowersave du Kicker (le tableau de bord de KDE). Une surveillance système complexe est exécutée par KSysguard. Lorsque vous utilisez GNOME, les fonctions décrites sont fournies par le moniteur ACPI (en tant qu'applet de tableau de bord) et le moniteur système.

KPowersave
: KPowersave est une applet qui affiche l'état de la batterie rechargeable dans le panneau de configuration. L'icône varie en fonction du type de source d'alimentation. Lorsque l'ordinateur est branché sur le secteur, une petite prise s'affiche. Lorsque vous travaillez en utilisant les batteries, l'icône se transforme en une pile. Le menu correspondant ouvre le module YaST de gestion de l'alimentation une fois que vous avez fourni le mot de passe root. Vous pouvez ainsi définir le comportement du système en fonction des différents types d'alimentation utilisés. Pour plus d'informations sur la gestion de l'alimentation et sur le module YaST correspondant, reportez-vous au Chapitre 21, *Gestion de l'alimentation* (p. 285).

KSysguard
: KSysguard est une application indépendante qui rassemble dans un seul environnement de surveillance tous les paramètres mesurables du système. KSysguard est doté d'un moniteur ACPI (état de la batterie), pour l'exploitation (la charge) de l'unité centrale, pour le réseau, pour le partitionnement et pour l'utilisation de la mémoire. Il peut également surveiller et afficher tous les processus système. Vous pouvez personnaliser la présentation et le filtrage des données collectées. Il est possible de surveiller différents paramètres système dans plusieurs pages de données ou de collecter les données de plusieurs ordinateurs en parallèle sur le réseau. Vous pouvez également exécuter KSysguard en tant que démon sur les ordinateurs dépourvus d'un environnement KDE. Pour plus d'informations sur ce programme, reportez-vous à sa fonction d'aide intégrée ou aux pages de manuel de SUSE.

Figure 18.2 *Surveillance de l'état de la batterie avec KSysguard*

Synchronisation des données

Lorsque vous travaillez en faisant la navette entre un ordinateur mobile déconnecté du réseau et un poste de travail mis en réseau dans un bureau, il est nécessaire d'assurer la synchronisation systématique des données traitées sur toutes vos instances. Cette opération peut aussi bien englober les dossiers de messages électroniques que les répertoires et les fichiers individuels dont vous avez besoin pour travailler lorsque vous êtes en déplacement ou au bureau. Dans les deux cas, la solution est la suivante :

Synchronisation de la messagerie électronique

Utilisez un compte IMAP pour stocker vos messages électroniques sur le réseau du bureau. Accédez ensuite à vos messages électroniques depuis votre poste de travail à l'aide d'un client de messagerie électronique IMAP (Mozilla Thunderbird Mail, Evolution ou KMail, par exemple), comme cela est décrit dans le guide de *démarrage*. Vous devez configurer le client de messagerie électronique pour toujours accéder au même dossier de `messages envoyés`. Cela garantit que tous les messages sont disponibles avec leurs informations d'état une fois le processus de synchronisation terminé. Utilisez un serveur SMTP mis en œuvre sur le client de messagerie d'envoi des messages plutôt que sur des serveurs Postfix ou Sendmail MTA à l'échelle du système, afin de recevoir des avertissements fiables quant aux messages non envoyés.

Synchronisation des fichiers et des répertoires

Il existe plusieurs utilitaires appropriés pour synchroniser des données entre un ordinateur portable et un poste de travail. Pour plus d'informations, reportez-vous au Chapitre 47, *Synchronisation des fichiers* (p. 785).

Communications sans fil

En plus de relier un ordinateur portable à un réseau privé ou professionnel à l'aide d'un câble, vous pouvez le connecter sans fil à d'autres ordinateurs, périphériques, téléphones cellulaires ou assistants personnels. Linux prend en charge trois types de communication sans fil.

WLAN
Parmi les technologies sans fil, WLAN est celle qui a la plus longue portée et qui est la seule adaptée aux réseaux de grande taille, voire aux réseaux parfois physiquement séparés dans l'espace. Des ordinateurs individuels peuvent se connecter les uns aux autres pour former un réseau sans fil indépendant ou pour accéder à Internet. Des périphériques appelés « points d'accès » jouent le rôle de stations de base pour les périphériques WLAN et d'intermédiaires pour l'accès à Internet. Un utilisateur mobile peut passer d'un point d'accès à un autre, en fonction de leur emplacement et de celui qui offre la meilleure connexion. Comme dans la téléphonie cellulaire, un vaste réseau est disponible pour les utilisateurs WLAN sans qu'ils soient liés à un emplacement spécifique pour accéder à ce réseau. Pour plus d'informations sur les réseaux WLAN, reportez-vous à la Section 22.1, « Réseau local sans fil » (p. 311).

Bluetooth
De toutes les technologies sans fil, c'est Bluetooth qui a le plus vaste spectre d'applications. Vous pouvez l'utiliser tout comme la technologie IrDA pour la communication entre des ordinateurs (portables) et des assistants personnels (PDA) ou des téléphones cellulaires. Vous pouvez également l'utiliser pour relier plusieurs ordinateurs dans la limite où chacun d'entre eux est visible des autres. En outre, vous pouvez vous servir de Bluetooth pour connecter des composants système sans fil, comme un clavier ou une souris. La portée de cette technologie reste toutefois insuffisante pour connecter des systèmes distants à un réseau. Choisissez la technologie WLAN pour des communications devant franchir des obstacles physiques tels que des murs. Pour plus d'informations à propos de la technologie Bluetooth, de ses applications et de sa configuration, reportez-vous à la Section 22.2, « Bluetooth » (p. 322).

IrDA
IrDA est la technologie sans fil dotée de la plus courte portée. Les deux parties en communication doivent être visibles l'une de l'autre. Il est impossible de surmonter des obstacles tels que des murs. Parmi les applications possibles de la technologie IrDA, vous avez la transmission d'un fichier d'un ordinateur portable vers un

téléphone cellulaire. La technologie IrDA couvre la courte distance entre l'ordinateur portable et le téléphone cellulaire. Le réseau mobile prend ensuite le relais pour le transport longue distance du fichier vers son destinataire. Une autre application de la technologie IrDA est la transmission sans fil des travaux d'impression au bureau. Pour plus d'informations sur la technologie IrDA, reportez-vous à la Section 22.3, « Transmission de données infrarouge » (p. 334).

18.1.4 Sécurité des données

Dans l'idéal, vous protégez de différentes façons vos données sur votre ordinateur portable contre les accès non autorisés. Des mesures de sécurité peuvent être prises dans les domaines suivants :

Protection contre le vol
Protégez systématiquement votre système contre le vol physique. Divers outils de sécurité, comme des chaînes, sont disponibles dans le commerce.

Sécurisation des données sur le système
Les données importantes doivent non seulement être chiffrées au cours de leur transmission, mais également sur le disque dur. Ainsi, leur protection est assurée en cas de vol. La création d'une partition chiffrée avec SUSE Linux est décrite à la Section 23.3, « Codage des partitions et des fichiers » (p. 358).

IMPORTANT: Sécurité des données et mise en veille sur disque

Les partitions chiffrées ne sont pas démontées pendant un événement de mise en veille sur disque. N'importe quelle personne qui parvient à dérober l'ordinateur et à exécuter une reprise du disque dur a donc accès à toutes les données de ces partitions.

Sécurité réseau
Vous devez sécuriser tout transfert de données, indépendamment de son mode de déroulement. Pour plus d'informations sur les problèmes généraux de sécurité sous Linux et sur les réseaux, reportez-vous à la Section 23.4, « Sécurité et confidentialité » (p. 362). Des mesures de sécurité en relation avec la mise en réseau sans fil sont disponibles au Chapitre 22, *Communications sans fil* (p. 311).

18.2 Matériel mobile

SUSE Linux prend en charge la détection automatique des périphériques de stockage mobiles via la technologie Firewire (IEEE 1394) ou USB. Le terme *périphérique mobile de stockage* s'applique aux disques durs Firewire ou USB, aux lecteurs Flash USB et aux appareils photo numériques de toute sorte. Dès que vous connectez ces périphériques au système via l'interface correspondante, la fonction d'enfichage à chaud les détecte et les configure automatiquement. subfs et submount garantissent que les périphériques sont montés aux emplacements correspondants dans le système de fichiers. L'utilisateur est ainsi complètement libéré du montage et du démontage manuel qu'il devait effectuer avec les précédentes versions de SUSE Linux. Un périphérique peut simplement être déconnecté dès qu'aucun programme n'accède plus à ce périphérique.

Disques durs externes (USB et Firewire)

Dès qu'un disque dur externe a été correctement reconnu par le système, son icône apparaît dans la liste des lecteurs montés dans *Poste de travail* (KDE et GNOME). Cliquez sur cette icône pour afficher le contenu du lecteur. Il est possible de créer des dossiers et des fichiers à cet emplacement, de les modifier ou de les supprimer. Pour renommer un disque dur en utilisant le nom que le système lui a donné, sélectionnez l'option correspondante dans le menu qui s'ouvre lorsque vous cliquez avec le bouton droit de la souris sur l'icône. Ce changement de nom s'affiche uniquement dans le gestionnaire de fichiers. Le descripteur grâce auquel le périphérique est monté dans `/media/usb-xxx` ou dans `/media/ieee1394-xxx` n'est pas affecté par ce changement.

Lecteurs Flash USB

Ces périphériques sont gérés par le système comme des disques durs externes. De la même manière, il est possible de renommer les entrées correspondantes dans le gestionnaire de fichiers.

Appareils photo numériques (USB et Firewire)

Les appareils photo numériques reconnus par le système apparaissent également en tant que lecteurs externes dans la fenêtre du gestionnaire de fichiers. KDE permet de lire les images et d'y accéder via l'adresse URL`camera:/`. Vous pouvez ensuite traiter ces images à l'aide de Digikam ou de GIMP. Lorsque vous utilisez GNOME, Nautilus affiche les images dans leur dossier respectif. f-spot est un utilitaire de traitement et de gestion simples des images. Pour un traitement avancé des photos, utilisez GIMP. Pour plus d'informations sur les appareils photo numériques et la

gestion des images, reportez-vous au Chapitre 15, *Appareils photo numériques et Linux* (p. 217).

18.3 Téléphones cellulaires et assistants personnels

Un système de bureau ou un ordinateur portable peuvent communiquer avec un téléphone cellulaire via la technologie Bluetooth ou IrDA. Certains modèles prennent en charge ces deux protocoles et d'autres uniquement l'un d'entre eux. Les domaines d'utilisation de ces deux protocoles et la documentation détaillée correspondante ont déjà été mentionnées à la section intitulée « Communications sans fil » (p. 265). Pour obtenir la configuration de ces protocoles sur les téléphones cellulaires, reportez-vous au manuel de ces dispositifs. Leur configuration du côté de Linux est décrite à la Section 22.2, « Bluetooth » (p. 322) et à la Section 22.3, « Transmission de données infrarouge » (p. 334).

La prise en charge de la synchronisation des données avec des dispositifs de poche fabriqués par Palm, Inc., est déjà intégrée à Evolution et à Kontact. La connexion initiale avec le périphérique est, dans les deux cas, facilement exécutée à l'aide d'un Assistant. Une fois la prise en charge de Palm Pilot configurée, il est nécessaire de déterminer le type de données à synchroniser (adresses, rendez-vous, etc.). Ces deux applications de groupe sont décrites dans le guide de *démarrage*.

Le programme KPilot intégré à Kontact est également disponible comme utilitaire indépendant. Il est décrit dans le guide de *démarrage*. Vous pouvez également utiliser le programme KitchenSync pour synchroniser les données des adresses.

18.4 Pour plus d'informations

Le point de référence central pour toutes les questions concernant les périphériques mobiles et Linux est le site `http://tuxmobil.org/`. Diverses sections de ce site Web traitent des aspects matériels et logiciels des ordinateurs portables, des assistants personnels, des téléphones cellulaires et des autres matériels mobiles.

Une approche comparable à celle de http://tuxmobil.org/ est disponible à l'adresse http://www.linux-on-laptops.com/. Pour obtenir des informations sur les ordinateurs portables et les dispositifs de poche, reportez-vous à ce site.

SUSE assure le développement d'une liste de diffusion en allemand, dédiée aux ordinateurs portables. (voir http://lists.suse.com/archive/suse-laptop/). Dans cette liste, les utilisateurs et les développeurs discutent de tous les aspects de l'informatique mobile sous SUSE Linux. Les questions posées en anglais obtiennent des réponses, mais la majorité des informations archivées ne sont disponibles qu'en allemand.

En cas de problème avec la gestion de l'alimentation des ordinateurs portables sous SUSE Linux, nous vous conseillons de vous reporter au fichier LISEZMOI situé dans le répertoire /usr/share/doc/packages/powersave. Ce répertoire contient souvent les commentaires de dernière minute des testeurs et des développeurs : vous y trouverez des astuces précieuses pour résoudre vos problèmes.

19 PCMCIA

Cette section traite des caractéristiques spécifiques du matériel et du logiciel PCMCIA utilisés pour les ordinateurs portables. PCMCIA signifie *Personal Computer Memory Card International Association* (Association internationale des éditeurs de carte mémoire pour PC) et est utilisé comme terme collectif pour tout ce qui concerne le matériel et le logiciel PCMCIA.

19.1 Matériel

Le composant le plus important est la carte PCMCIA. Il existe deux types de cartes PCMCIA :

Cartes PC
Ces cartes ont vu le jour en même temps que le format PCMCIA. Elles utilisent un bus 16 bits pour la transmission des données et sont souvent assez bon marché. Certains ponts PCMCIA récents éprouvent des difficultés à détecter ces cartes. Néanmoins, une fois détectées, elles fonctionnent généralement très bien et ne posent aucun problème.

Cartes CardBus
Il s'agit d'une norme plus récente. Elles utilisent un bus 32 bits, qui les rend plus rapides mais également plus onéreuses. Elles sont intégrées au système, comme les cartes PCI, et fonctionnent très bien.

Le second composant important est le contrôleur PCMCIA (ou carte PC ou pont CardBus), qui établit la connexion entre la carte et le bus PCI. Tous les modèles courants

sont pris en charge. S'il s'agit d'un périphérique PCI intégré, la commande `lspci -vt` fournit des informations complémentaires.

19.2 Logiciel

Avec le kernel actuel, les ponts et les cartes PCMCIA sont gérés par le sous-système d'enfichage à chaud. Il existe des événements `pcmcia_socket` pour chaque pont et événement `pcmcia`. La commande udevd charge tous les modules nécessaires et appelle les outils permettant de configurer ces périphériques. Ces actions sont définies dans le fichier `/etc/udev/rules.d/`.

`/etc/pcmcia/config.opts` est utilisé pour la configuration des ressources. Le pilote adapté est déterminé par les tables de périphériques figurant dans les pilotes. Les informations relatives à l'état actuel des sockets et des cartes apparaissent dans le fichier `/sys/class/pcmcia_socket/` et via la commande `pccardctl`.

Du fait de l'évolution constante du système PCMCIA, cette documentation est incomplète. Pour obtenir une présentation complète, reportez-vous au fichier `/usr/share/doc/packages/pcmciautils/README.SUSE`.

Gestion du profil de configuration du système (SCPM, System Configuration Profile Management) 20

La gestion SCPM (system configuration profile management, gestion du profil de configuration du système) vous permet d'adapter la configuration de votre ordinateur à différents systèmes d'exploitation et à différentes configurations matérielles. Elle gère un jeu de profils système pour les différents scénarios. Elle permet également de passer facilement d'un profil à l'autre sans reconfigurer manuellement le système.

Dans certains cas, la configuration du système doit être modifiée. Les ordinateurs portables sont les premiers concernés, puisqu'ils peuvent être utilisés depuis des endroits divers. La gestion SCPM est également utile si un ordinateur de bureau doit fonctionner provisoirement avec une configuration matérielle modifiée. Il doit être facile de restaurer la configuration initiale du système, mais aussi de reproduire les modifications effectuées. Grâce à SCPM, toute configuration peut être conservée dans un profil personnalisé.

Le principal champ d'application de SCPM reste la configuration réseau des ordinateurs portables. En effet, les changements de configuration réseau se répercutent souvent sur d'autres services (par exemple, les messageries électroniques ou les proxy). D'autres éléments changent également : imprimantes différentes pour la maison et le bureau, configuration de serveur X personnalisée pour le projecteur multimédia utilisé lors de conférences, paramètres d'économie d'énergie adaptés aux déplacements, fuseau horaire différent pour une filiale à l'étranger.

20.1 Terminologie

Les termes ci-dessous sont utilisés dans la documentation SCPM et le module YaST.

- Le terme *configuration du système* désigne la configuration complète de l'ordinateur. Il couvre tous les paramètres fondamentaux, notamment l'utilisation des partitions de disque dur, les paramètres réseau, la sélection du fuseau horaire et la configuration réseau.

- Un *profil* (ou *profil de configuration*) est un état qui a été sauvegardé et qui peut être restauré à tout moment.

- Le *profil actif* est le dernier profil sélectionné. Cela ne signifie pas que la configuration actuelle du système correspond exactement à ce profil. Elle peut en effet être modifiée à tout moment.

- Dans le contexte de SCPM, on appelle *ressource* un élément de la configuration du système. Cet élément peut être un fichier ou un lien symbolique incluant des méta-données (comme le nom de l'utilisateur), des autorisations ou un temps d'accès. Il peut également s'agir d'un service système exécuté dans ce profil, mais désactivé dans un autre.

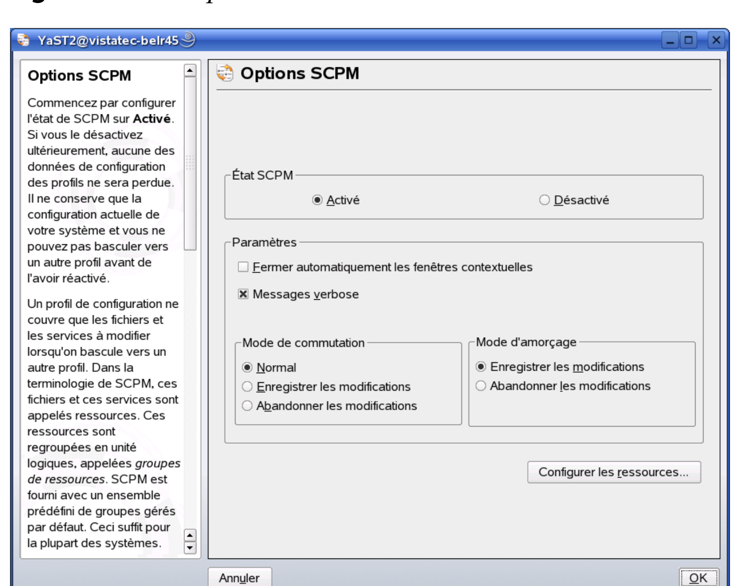
- Chaque ressource appartient à un *groupe de ressources* donné. Chaque groupe contient toutes les ressources qui doivent être réunies de façon logique. Ainsi, un groupe peut contenir un service et ses fichiers de configuration. Il est très facile de grouper des ressources gérées par SCPM. Aucune connaissance particulière des fichiers de configuration du service désiré n'est requise. SCPM comprend un certain nombre de groupes de ressources préconfigurés, qui doivent suffire dans la plupart des cas.

20.2 Utilisation du gestionnaire de profils YaST

Pour démarrer le gestionnaire de profils YaST, cliquez sur *Système* → *Gestionnaire de profils* dans le centre de configuration YaST. Au premier démarrage, pour activer SCPM de manière explicite, sélectionnez *Activé* dans la boîte de dialogue *Options SCPM*, illustrée à la Figure 20.1, « Options SCPM YaST » (p. 275). Dans *Paramètres*, indiquez

si les fenêtres contextuelles de progression doivent être fermées automatiquement et si les messages verbose concernant l'avancement de votre configuration SCPM doivent s'afficher. Dans la zone *Mode de commutation*, indiquez si les ressources modifiées pour le profil actif doivent être enregistrées ou ignorées lors du basculement entre profils. Si le *Mode de commutation* est défini sur *Normal*, toutes les modifications apportées au profil actif sont enregistrées lors du basculement. Pour définir le comportement de SCPM au démarrage, choisissez *Enregistrer les modifications* (paramètre par défaut) ou *Abandonner les modifications* dans la zone *Mode d'amorçage*.

Figure 20.1 *Options SCPM YaST*

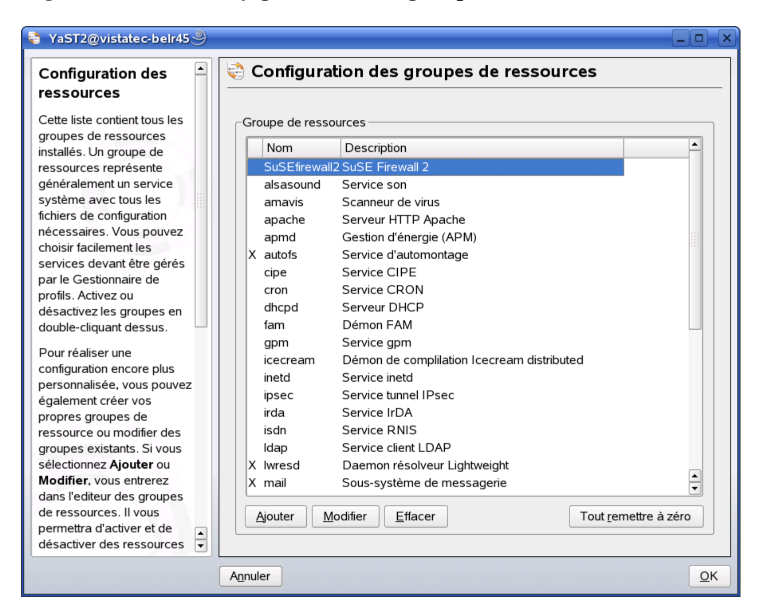


20.2.1 Configuration des groupes de ressources

Pour apporter des modifications à la configuration en cours des ressources, choisissez *Configurer les ressources* dans la boîte de dialogue *Options SCPM*. La boîte de dialogue qui s'affiche ensuite (voir la Figure 20.2, « Configuration des groupes de ressources » (p. 276)) répertorie tous les groupes de ressources disponibles sur votre système. Pour ajouter ou modifier un groupe de ressources, définissez ou modifiez les informations des colonnes *Groupe de ressources* et *Description*. Pour un service LDAP, par exemple,

entrez `ldap` comme *Groupe de ressources* et `Service client LDAP` comme *Description*. Entrez ensuite les ressources appropriées (services, fichiers de configuration ou les deux) ou modifiez les ressources existantes. Supprimez les ressources inutilisées. Pour réinitialiser l'état des ressources sélectionnées, c'est-à-dire ignorer les modifications qui leur ont été apportées et revenir aux valeurs initiales, choisissez *Rétablir le groupe*. Les modifications sont enregistrées dans le profil actif.

Figure 20.2 *Configuration des groupes de ressources*



20.2.2 Création d'un profil

Pour créer un profil, cliquez sur *Ajouter* dans la première boîte de dialogue (*Gestion des profils de configuration système*). Dans la fenêtre qui s'ouvre, choisissez de baser le nouveau profil sur la configuration actuelle du système (SCPM extrait automatiquement la configuration en cours et l'écrit dans votre profil) ou sur un profil existant. Si vous basez le nouveau profil sur la configuration actuelle du système, vous pouvez faire de ce nouveau profil le profil actif. Aucune modification n'est apportée à l'ancien profil et aucun service n'est démarré ni arrêté.

Dans la boîte de dialogue suivante, fournissez un nom et une courte description pour le nouveau profil. Pour que SCPM exécute des scripts spéciaux sur un jeu de profils,

entrez le chemin de chaque exécutable (voir Figure 20.3, « Paramètres spéciaux du profil » (p. 277)). Pour plus d'informations, consultez la Section 20.3.4, « Paramètres avancés du profil » (p. 281). SCPM vérifie les ressources du nouveau profil. Une fois cette vérificafion effectuée, le nouveau profil est prêt à être utilisé.

Figure 20.3 *Paramètres spéciaux du profil*

20.2.3 Modification des profils existants

Pour modifier un profil, cliquez sur *Modifier* dans la première boîte de dialogue (*Gestion des profils de configuration système*). Modifiez ensuite le nom, la description, les scripts et les ressources en fonction de vos besoins.

20.2.4 Passage d'un profil à un autre

Pour changer de profil, ouvrez le gestionnaire de profils Le profil actif est marqué par une flèche. Sélectionnez le profil à ouvrir, puis cliquez sur *Basculer vers*. SCPM recherche les ressources nouvelles ou modifiées et les ajoute, le cas échéant.

Si une ressource a été modifiée, YaST ouvre la boîte de dialogue *Confirmer la commutation*. La liste *Groupes de ressources modifiées du profil actif* répertorie tous les groupes de ressources du profil actif qui ont été modifiés, mais pas encore enregistrés dans le profil actif. *Enregistrer ou Ignorer* pour le groupe de ressources actuellement sélectionné détermine si les modifications apportées à ce groupe de ressources doivent être enregistrées dans le profil actif ou être ignorées. Vous pouvez également sélectionner chaque ressource et cliquer sur *Détails* pour analyser les modifications en détail. Une liste des fichiers de configuration ou des exécutables qui appartiennent au groupe de ressources et qui ont été modifiés s'affiche. Pour voir une comparaison ligne à ligne de l'ancienne et de la nouvelle version, cliquez sur *Afficher les modifications*. Après avoir analysé les modifications, décidez de ce que vous allez en faire dans *Action* :

Enregistrer la ressource
Enregistre la ressource dans le profil actif sans modifier les autres profils.

Ignorer la ressource
Laisse la ressource active intouchée. La modification est ignorée.

Enregistrer dans tous les profils
Copie la configuration entière de cette ressource dans tous les autres profils.

Patcher tous les profils
Applique uniquement les modifications les plus récentes à tous les profils.

Enregistrer ou Ignorer tout permet d'enregistrer ou d'ignorer les modifications apportées à toutes les ressources de la boîte de dialogue.

Une fois les modifications du profil actif confirmées, cliquez sur *OK* pour quitter la boîte de dialogue *Confirmer la commutation*. SCPM bascule vers le nouveau profil. Pendant le basculement, il exécute les scripts prestop et poststop sur l'ancien profil et les scripts prestart et poststart sur le nouveau profil.

20.3 Configuration de SCPM via la ligne de commande

Cette section présente la configuration de SCPM via la ligne de commande : elle indique comment le démarrer, le configurer et utiliser les profils.

20.3.1 Démarrage de SCPM et définition de groupes de ressources

Avant d'utiliser SCPM, vous devez l'activer. Pour ce faire, utilisez la commande `scpm enable` . Lors de sa première exécution, SCPM est initialisé, ce qui prend quelques secondes. Vous pouvez désactiver SCPM avec `scpm disable` à tout moment pour éviter le basculement inopportun entre profils. Si vous le réactivez par la suite, l'initialisation reprendra.

Par défaut, SCPM gère les paramètres réseau et imprimante ainsi que la configuration X.Org. Pour gérer les fichiers de configuration ou les services spéciaux, activez les groupes de ressources. Pour afficher la liste des groupes de ressources prédéfinis, utilisez `scpm list_groups` . Pour n'afficher que les groupes déjà activés, utilisez `scpm list_groups -a` . Pour exécuter ces commandes, vous devez être connecté en tant que `root`.

```
scpm list_groups -a

nis                  Network Information Service client
mail                 Mail subsystem
ntpd                 Network Time Protocol daemon
xf86                 X Server settings
autofs               Automounter service
network              Basic network settings
printer              Printer settings
```

Pour activer ou désactiver un groupe, utilisez `scpm activate_group NAME` ou `scpm deactivate_group NAME` (remplacez `NAME` par le nom du groupe).

20.3.2 Création et gestion de profils

Lorsque SCPM est activé, il existe déjà un profil nommé `default`. Vous pouvez afficher la liste des profils disponibles avec `scpm list` . Le profil existant est également le profil actif, comme vous pouvez le vérifier avec `scpm active` . Le profil `default` est une configuration de base de laquelle sont dérivés les autres profils. C'est pourquoi vous devez d'abord définir les paramètres qui seront identiques dans tous les profils. Enregistrez ensuite ces modifications dans le profil actif à l'aide de `scpm reload` . Vous pouvez copier et renommer le profil `default` afin de l'utiliser comme base des nouveaux profils.

Vous pouvez ajouter un nouveau profil de deux manières différentes. Si le nouveau profil (appelé ici `work`) doit être basé sur le profil `default`, créez-le avec `scpm copy default work` . La commande `scpm switch work` bascule vers le nouveau profil, qui peut alors être modifié. Vous souhaiterez peut-être modifier la configuration du système à des fins particulières et enregistrer les modifications dans un nouveau profil. La commande `scpm add work` crée un profil en enregistrant la configuration actuelle du système dans le profil `work` et en l'activant. Exécutez alors `scpm reload` pour enregistrer les modifications apportées au profil `work`.

Les commandes `scpm rename x y` et `scpm delete z` vous permettent de renommer et de supprimer des profils. Ainsi, pour renommer `work` en `project`, entrez `scpm rename work project` . Pour supprimer le profil `project`, entrez `scpm delete project` . Le profil actif ne peut pas être supprimé.

20.3.3 Changement de profil de configuration

La commande `scpm switch work` permet de basculer vers un autre profil (le profil `work`, dans ce cas). Basculez vers le profil actif pour y intégrer les paramètres modifiés de la configuration du système. Cette opération est équivalente à la commande `scpm reload` .

Lors du basculement entre les profils, SCPM commence par vérifier quelles ressources ont été modifiées pour le profil actif. Il demande ensuite si la modification de chaque ressource doit être ajoutée au profil actif ou être ignorée. Si vous préférez avoir une liste séparée des ressources (comme dans les anciennes versions de SCPM), utilisez la commande switch avec le paramètre `-r` : `scpm switch -r work` .

```
scpm switch -r work

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

SCPM compare alors la configuration en cours du système avec le profil vers lequel il doit basculer. À cette phase, SCPM identifie les services système à arrêter ou à redémarrer en raison de dépendances mutuelles ou des modifications de la configuration. Cette opération s'apparente à un redémarrage partiel du système, car seule une partie du système redémarre alors que le reste continue de fonctionner. Enfin, les services

système sont arrêtés, les ressources modifiées, comme les fichiers de configuration, sont écrits, et les services système sont redémarrés.

20.3.4 Paramètres avancés du profil

Vous pouvez entrer une description pour chaque profil affiché avec `scpm list` . Pour le profil actif, utilisez `scpm set description "text"` . Pour les profils inactifs, indiquez le nom du profil, par exemple `scpm set description "text" work` . Il est parfois utile d'effectuer des actions supplémentaires non proposées par SCPM lors du basculement entre les profils. Vous pouvez rattacher jusqu'à quatre exécutables à chaque profil. Ils sont appelés à différentes étapes du basculement. Ces étapes sont les suivantes :

prestop
avant l'arrêt des services, lors de la fermeture du profil

poststop
après l'arrêt des services, lors de la fermeture du profil

prestart
avant le démarrage des services, lors de l'activation du profil

poststart
après le démarrage des services, lors de l'activation du profil

Ajoutez ces actions à l'aide de la commande `set`, en entrant `scpm set prestop filename` , `scpm set poststop filename` , `scpm set prestart filename` ou `scpm set poststart filename` . Les scripts doivent être exécutables et faire référence au bon interpréteur.

AVERTISSEMENT: Intégration d'un script personnalisé

Les scripts supplémentaires que SCPM doit exécuter doivent être lisibles et exécutables par le superutilisateur (`root`). L'accès à ces fichiers doit être bloqué pour tous les autres utilisateurs. Entrez les commandes `chmod 700 filename` et `chown root:root filename` pour donner à `root` des autorisations exclusives sur ces fichiers.

Demandez tous les paramètres supplémentaires entrés avec `set` et `get`. La commande `scpm get poststart` , par exemple, renvoie le nom de l'appel poststart ou rien si rien n'a été associé. Réinitialisez ces paramètres en les remplaçant par `""`. La commande `scpm set prestop ""` supprime le programme prestop associé.

Toutes les commandes `set` et `get` peuvent être appliquées à un profil arbitraire de la même manière que les commentaires. Par exemple, `scpm get prestop filename work` ou `scpm get prestop work` .

20.4 Utilisation de l'applet Sélecteur de profil

Le sélecteur de profil du tableau de bord GNOME ou KDE permet de contrôler facilement les paramètres SCPM. Créez, modifiez ou supprimez des profils via YaST comme décrit à la Section 20.2, « Utilisation du gestionnaire de profils YaST » (p. 274) et changez de profil. Le changement de profil peut être effectué par un utilisateur normal à condition que l'administrateur du système l'autorise. Ouvrez le Sélecteur de profil depuis le menu de votre bureau à l'aide de *Système* → *Applet bureau* → *Sélecteur de profil*.

Pour autoriser les utilisateurs normaux à changer de profil, cliquez avec le bouton droit sur l'icône du Sélecteur de profil dans le tableau de bord, puis choisissez *Permettre la commutation utilisateur* dans le menu qui s'affiche. Saisissez le mot de passe root. Tous les utilisateurs de votre système peuvent maintenant basculer les profils.

Une fois que vous avez cliqué sur l'icône du Sélecteur de profil, tous les profils configurés dans YaST s'affichent, qu'ils aient été définis directement via un appel YaST ou via *Démarrer le module du gestionnaire de profils de YaST2*. Sélectionnez celui vers lequel vous souhaitez basculer à l'aide des touches du curseur. SCPM passe automatiquement au nouveau profil.

20.5 Dépannage

Cette section couvre les problèmes fréquents rencontrés avec SCPM. Elle vous explique comment ils peuvent se produire et comment vous pouvez les résoudre.

20.5.1 Interruption pendant le basculement

SCPM s'arrête parfois de fonctionner pendant le basculement. Ce problème peut avoir plusieurs origines : l'arrêt par un utilisateur, une panne de courant ou encore un problème avec SCPM. S'il se produit, un message d'erreur indiquant que SCPM est verrouillé s'affiche au redémarrage de SCPM. Cela a pour but de garantir la sécurité de votre système. En effet, les données stockées dans la base de données peuvent différer de l'état du système. Pour résoudre ce problème, exécutez `scpm recover` . SCPM effectue toutes les opérations qu'il n'avait pas pu réaliser lors de la précédente exécution. Vous pouvez également exécuter `scpm recover -b` , qui tente d'annuler toutes les opérations déjà effectuées lors de l'exécution précédente. Si vous utilisez le gestionnaire de profils YaST, vous pouvez afficher une boîte de dialogue de récupération au démarrage pour lancer les commandes décrites ci-dessus.

20.5.2 Modification de la configuration du groupe de ressources

Pour modifier la configuration du groupe de ressources après avoir initialisé SCPM, entrez `scpm rebuild` après avoir ajouté ou supprimé des groupes. Les nouvelles ressources sont alors ajoutées à tous les profils et les ressources supprimées sont définitivement effacées. Si les ressources supprimées sont configurées de manière différente en fonction du profil, ces données de configuration sont perdues, à l'exception de la version en cours dans votre système, que SCPM ne modifie pas. Si vous modifiez la configuration avec YaST, il est inutile d'entrer la commande de reconstruction : YaST la prend en charge.

20.6 Sélection d'un profil au démarrage du système

Pour sélectionner un profil au démarrage du système, appuyez sur F3 dans l'écran de démarrage. La liste des profils disponibles s'affiche. Utilisez les touches fléchées pour sélectionner un profil, puis confirmez votre sélection en appuyant sur Entrée. Le profil sélectionné est alors utilisé en tant qu'option de démarrage.

20.7 Pour plus d'informations

La documentation la plus récente est disponible dans les pages d'informations de SCPM (info scpm). Des informations destinées aux développeurs sont disponibles dans `/usr/share/doc/packages/scpm`.

21 Gestion de l'alimentation

Essentielle pour les ordinateurs portables, la gestion de l'alimentation est également utile sur d'autres systèmes. Deux technologies sont disponibles : APM (advanced power management, gestion avancée de l'alimentation) et ACPI (advanced configuration and power interface, interface d'alimentation et de configuration avancée). Il est également possible de contrôler la fréquence de l'unité centrale pour économiser l'énergie ou réduire le bruit. Ces options peuvent être configurées manuellement ou via un module YaST spécial.

Contrairement à la gestion APM, utilisée uniquement sur les ordinateurs portables, l'outil ACPI de configuration et d'information matérielle est disponible sur tous les ordinateurs modernes (portables, ordinateurs de bureau et serveurs). Toutes les technologies de gestion de l'alimentation nécessitent des routines BIOS et matérielles adaptées, disponibles sur la plupart des ordinateurs portables et sur de nombreux ordinateurs de bureau.

La gestion APM est utilisée sur les ordinateurs anciens. Cette technologie étant essentiellement composée d'un jeu de fonctions mis en oeuvre dans le BIOS, sa prise en charge varie en fonction du matériel. Le même problème se pose pour la norme ACPI, qui est encore plus complexe. C'est pourquoi il est pratiquement impossible de recommander l'une de ces technologies plutôt que l'autre. Testez les différentes procédures sur votre matériel, puis sélectionnez la technologie la mieux adaptée.

IMPORTANT: Gestion de l'alimentation des processeurs AMD64

Les processeurs AMD64 à kernel 64 bits ne prennent en charge que la gestion ACPI.

21.1 Fonctions d'économie d'énergie

Les fonctions d'économie d'énergie sont aussi importantes pour les ordinateurs de bureau que pour les portables. Les principales fonctions d'économie d'énergie et leur utilisation dans les systèmes de gestion de l'alimentation APM et ACPI sont décrites ci-dessous.

Mise en attente
Ce mode d'exploitation éteint l'affichage. Sur certains ordinateurs, il limite les performances du processeur. Cette fonction n'est disponible que dans certaines mises en oeuvre de la gestion APM. Elle correspond à l'état ACPI S1 ou S2.

Mise en veille (en mémoire)
Ce mode écrit l'état de l'ensemble du système dans la RAM, puis met en veille tout le système, excepté la RAM. Dans cet état, l'ordinateur consomme très peu d'énergie. Il est en mesure de reprendre le travail au point où il l'avait laissé en quelques secondes, sans redémarrer ni relancer les applications. Il est généralement possible de mettre en veille les périphériques qui utilisent la technologie APM en fermant le couvercle et de les réactiver en le rouvrant. Cette fonction correspond à l'état ACPI S3. Sa prise en charge est toujours en développement et dépend donc du matériel.

Hibernation (mise en veille sur disque)
Dans ce mode d'exploitation, l'état du système entier est écrit sur le disque dur, puis le système est désactivé. La réactivation demande 30 à 90 secondes. L'état précédant la suspension est restauré. Certains fabricants proposent des variantes hybrides de ce mode (par exemple, RediSafe sur les Thinkpad IBM). Cette fonction correspond à l'état ACPI S4. Sous Linux, elle est contrôlée par des routines de kernel indépendantes des technologies APM et ACPI.

Moniteur de charge de la batterie
Les systèmes ACPI et APM contrôlent le niveau de charge de la batterie et fournissent des informations sur ce niveau. Ils coordonnent les actions à effectuer lorsque la charge de la batterie atteint un niveau critique.

Mise hors tension automatique
Après un arrêt, l'ordinateur est mis hors tension. Cette fonction est particulièrement importante lorsque l'ordinateur a été arrêté automatiquement alors que la batterie était presque déchargée.

Arrêt des composants système

La réduction de la consommation électrique du système repose essentiellement sur l'arrêt du disque dur. Selon la fiabilité du système, le disque dur peut être mis en veille pendant un certain temps. Toutefois, le risque de perte de données s'accroît avec la durée de la veille. Les autres composants peuvent être désactivés via ACPI (du moins en théorie), ou définitivement arrêtés via le BIOS.

Contrôle de la vitesse du processeur

Il existe trois manières d'économiser l'énergie au niveau de l'unité centrale : mettre en veille du processeur (états C), limiter son utilisation et contrôler sa fréquence et de sa tension (technologie PowerNow! ou Speedstep). Selon le mode d'exploitation de l'ordinateur, ces méthodes peuvent également être combinées.

21.2 APM

Certaines fonctions de gestion de l'alimentation sont assurées par le BIOS APM lui-même. Sur de nombreux ordinateurs portables, les modes de mise en attente et en veille sont activés par des combinaisons de touches ou par la fermeture du couvercle, sans intervention spécifique du système d'exploitation. Cependant, pour activer ces modes à l'aide d'une commande, certaines actions doivent être déclenchées avant la mise en attente du système. Pour afficher le niveau de charge de la batterie, vous avez besoin de paquetages de programmes spécifiques et d'un kernel adapté.

Les kernels SUSE Linux comportent une prise en charge APM intégrée. Cependant, la gestion APM n'est activée qu'en l'absence de fonction ACPI dans le BIOS, si un BIOS APM est détecté. Pour activer la gestion APM, il faut désactiver ACPI en entrant `acpi=off` à l'invite de démarrage. Pour vérifier si ACPI est actif, entrez `cat /proc/apm`. Une sortie composée de plusieurs chiffres indique que tout va bien. Vous pouvez alors éteindre l'ordinateur avec la commande `shutdown -h`.

Les mises en oeuvre de BIOS non conformes aux normes provoquent des problèmes de gestion APM. Il est possible de prévenir certains de ces problèmes à l'aide de paramètres de démarrage spéciaux. Tous les paramètres sont saisis à l'invite de commande sous la forme `apm=parameter` :

on ou off

La prise en charge APM est activée ou désactivée.

(no-)allow-ints
L'exécution des fonctions du BIOS peut être interrompue.

(no-)broken-psr
La fonction « GetPowerStatus » du BIOS ne fonctionne pas.

(no-)realmode-power-off
Le processeur est réinitialisé en mode réel avant son arrêt.

(no-)debug
Les événements APM sont enregistrés dans le journal système.

(no-)power-off
Le système est mis hors tension après son arrêt.

bounce-interval=*n*
Temps, en centièmes de seconde, pendant lequel les suspensions qui suivent une suspension initiale sont ignorées.

idle-threshold=*n*
Niveau d'activité du système à partir duquel la fonction BIOS `idle` s'exécute (0=jamais, 100=toujours).

idle-period=*n*
Temps, en centièmes de seconde, au bout duquel l'activité du système est mesurée.

Le démon APM (apmd) n'est plus utilisé. Ses fonctions sont désormais gérées par powersaved, qui contrôle la fréquence de l'unité centrale et assure la gestion ACPI.

21.3 ACPI

La gestion ACPI (advanced configuration and power interface, interface d'alimentation et de configuration avancée) donne au système d'exploitation la possibilité de configurer et de contrôler les composants matériels. Elle remplace PnP et APM. Elle fournit des informations sur la batterie, l'adaptateur secteur, la température, le ventilateur et les événements systèmes tels que « la fermeture du couvercle » ou « le niveau de la batterie ».

Le BIOS fournit, dans des tables, des informations sur les différents composants et les modes d'accès au matériel. Le système d'exploitation utilise ces informations, entre autres, pour affecter les interruptions ou activer et désactiver les composants. Le système d'exploitation exécutant des commandes stockées dans le BIOS, les fonctions disponibles dépendent du BIOS. Le système ACPI peut détecter et charger les tables répertoriées dans `/var/log/boot.msg`. Reportez-vous à la Section 21.3.4, « Dépannage » (p. 294) pour plus d'informations sur le dépannage des problèmes ACPI.

21.3.1 ACPI en action

Si le kernel détecte un BIOS ACPI au démarrage du système, ACPI est automatiquement activé et APM désactivé. Sur les machines plus anciennes, le paramètre de démarrage `acpi=force` peut être nécessaire. L'ordinateur doit prendre en charge ACPI 2.0 ou une version ultérieure. Pour savoir si ACPI a été activé, consultez les messages de démarrage du kernel dans `/var/log/boot.msg`.

Un certain nombre de modules doit ensuite être chargé par le script de démarrage du démon powersave. Si l'un de ces modules provoque des problèmes, il est possible d'exclure son chargement/déchargement dans `/etc/sysconfig/powersave/common`. Le journal système (`/var/log/messages`) stocke les messages des modules. Il permet donc d'identifier les modules détectés.

Le répertoire `/proc/acpi` contient plusieurs fichiers qui fournissent des informations sur l'état du système ou qui permettent de modifier certains états. Certaines fonctions dont le développement n'est pas achevé sont toujours indisponibles ou inefficaces ; en outre, la prise en charge des différentes fonctions dépend fortement du BIOS mis en oeuvre par le fabricant.

Tous les fichiers, excepté `dsdt` et `fadt`, sont lisibles dans `cat`. Certains contiennent des paramètres modifiables à l'aide de la commande `echo` ; par exemple, `echo X > file` permet de spécifier des valeurs correctes pour X. Utilisez toujours la commande `powersave` pour accéder à ces informations et aux options de contrôle. Les fichiers les plus importants sont décrits ci-dessous.

`/proc/acpi/info`
Informations générales sur la gestion ACPI.

/proc/acpi/alarm
Spécifie les circonstances dans lesquelles le système doit quitter un état de veille (cette fonctionnalité n'est actuellement pas prise en charge).

/proc/acpi/sleep
Informations sur les états de veille possibles.

/proc/acpi/event
Répertorie tous les événements. Ces événements sont traités par le démon Powersave (`powersaved`). Si aucun démon n'accède à ce fichier, les événements tels qu'un appui bref sur le bouton d'alimentation ou la fermeture du couvercle peuvent être lus via `cat /proc/acpi/event` (arrêté via Ctrl + C).

/proc/acpi/dsdt et /proc/acpi/fadt
Ces fichiers contiennent les tables ACPI DSDT (differentiated system description table) et FADT (fixed ACPI description table). Ils peuvent être lus à l'aide des programmes `acpidmp`, `acpidisasm` et `dmdecode`, disponibles, avec leur documentation, dans le paquetage `pmtools`. Par exemple, `acpidmp DSDT | acpidisasm`.

/proc/acpi/ac_adapter/AC/state
Indique si l'adaptateur secteur est connecté.

/proc/acpi/battery/BAT*/{alarm,info,state}
Informations détaillées sur l'état de la batterie. Pour connaître le niveau de charge, comparez la `dernière capacité complète` indiquée dans `info` à la `capacité restante` figurant dans `state`. Il est plus facile de connaître le niveau de charge en utilisant les programmes spéciaux présentés à la Section 21.3.3, « Outils ACPI » (p. 294). Le niveau de charge qui déclenche un événement de batterie peut être spécifié dans `alarm`.

/proc/acpi/button
Ce répertoire contient des informations sur divers paramètres.

/proc/acpi/fan/FAN/state
Indique si le ventilateur est actif. Vous pouvez activer ou désactiver manuellement le ventilateur en écrivant `0` (on) ou `3` (off) dans ce fichier. Toutefois, le code ACPI du kernel et le matériel (ou le BIOS) ignorent ce paramètre si la température dépasse un certain niveau.

/proc/acpi/processor/*
Un sous-répertoire séparé est utilisé pour chaque unité centrale de votre système.

/proc/acpi/processor/*/info
Informations sur les options d'économie d'énergie du processeur.

/proc/acpi/processor/*/power
Informations sur l'état actuel du processeur. Un astérisque en regard de `C2` indique que le processeur est inactif. Il s'agit de l'état le plus fréquent, comme l'indique la valeur `usage`.

/proc/acpi/processor/*/throttling
Permet de définir la limitation de l'horloge du processeur. D'ordinaire, huit niveaux de limitation sont proposés. La limitation est indépendante du contrôle de la fréquence.

/proc/acpi/processor/*/limit
Si les performances (obsolète) et la limitation de l'utilisation du processeur sont contrôlées automatiquement par un démon, ce fichier permet de définir les limites maximum. Certaines de ces limites sont déterminées par le système, d'autres peuvent être ajustées par l'utilisateur.

/proc/acpi/thermal_zone/
Ce dossier comporte un sous-répertoire pour chaque zone thermique. Une zone thermique est une zone qui présente des propriétés thermiques uniformes ; les noms et les numéros des zones thermiques sont fixés par le fabricant du matériel. La gestion ACPI offre de nombreuses possibilités de gestion de la température, dont beaucoup sont rarement mises en oeuvre. La température est contrôlée de manière conventionnelle par le BIOS. Le système d'exploitation intervient peu, la durée de vie du matériel étant en jeu. Certains fichiers n'ont donc qu'une valeur théorique.

/proc/acpi/thermal_zone/*/temperature
Température actuelle de la zone thermique.

/proc/acpi/thermal_zone/*/state
Indique si tout est `ok` ou si ACPI applique un refroidissement `actif` ou `passif`. Lorsque le contrôle des ventilateurs est assuré par des fonctions indépendantes de la gestion ACPI, l'état est toujours `ok`.

/proc/acpi/thermal_zone/*/cooling_mode
Sélectionnez le refroidissement contrôlé par ACPI : refroidissement passif (moins performant, mais plus économique) ou actif (plus performant, mais générant un bruit de ventilateur plus important).

/proc/acpi/thermal_zone/*/trip_points
Permet la détermination des limites de température qui déclenchent des actions spécifiques, comme le refroidissement passif ou actif, l'interruption (`hot`) ou l'arrêt (`critical`). Les actions possibles sont définies dans la table DSDT (dépendant du périphérique). La norme ACPI définit les points de déclenchement `critical`, `hot`, `passive`, `active1` et `active2` ; même si ces points ne sont pas tous mis en oeuvre, ils doivent tous être entrés dans ce fichier dans cet ordre. Ainsi, l'entrée `echo 90:0:70:0:0 > trip_points` règle le point de déclenchement `critical` à `90` et le point de déclenchement `passive` à `70` (toutes les températures étant mesurées en degrés Celsius).

/proc/acpi/thermal_zone/*/polling_frequency
Permet de modifier le mode d'interrogation si la valeur `temperature` n'est pas automatiquement mise à jour lorsque la température change. La commande `echo X > /proc/acpi/thermal_zone/*/polling_frequency` impose une lecture de la température toutes les `X` secondes. Pour désactiver l'interrogation, définissez `X=0`.

En principe, il est inutile d'éditer manuellement aucun de ces paramètres, informations et événements. Le démon Powersave (powersaved) et d'autres applications, comme powersave, kpowersave et wmpowersave, peuvent effectuer les modifications nécessaires (voir Section 21.3.3, « Outils ACPI » (p. 294)). powersaved couvrant les fonctionnalités de acpid, celui-ci n'est plus nécessaire.

21.3.2 Contrôle des performances de l'unité centrale

Trois méthodes différentes permettent d'économiser l'énergie au niveau de l'unité centrale. Selon le mode d'exploitation de l'ordinateur, ces méthodes peuvent être combinées. Le fait d'économiser l'énergie signifie que le système chauffe moins et que les ventilateurs sont moins souvent activés.

Contrôle de la fréquence et de la tension

Les technologies AMD et Intel de contrôle de la fréquence et de la tension sont appelées, respectivement, PowerNow! et Speedstep, mais elles ne sont pas les seules du marché : des technologies équivalentes sont appliquées par les processeurs d'autres fabricants. La fréquence d'horloge de l'unité centrale et sa tension principale sont réduites simultanément, ce qui permet des économies d'énergie plus que linéaires. Ainsi, lorsque la fréquence et les performances sont réduites de moitié, la consommation d'énergie est réduite de plus de 50 %. Cette technologie est indépendante de la gestion APM ou ACPI ; elle nécessite un démon qui adapte la fréquence aux besoins de performances. Ces paramètres peuvent être définis dans le répertoire `/sys/devices/system/cpu/cpu*/cpufreq/`.

Limitation de la fréquence d'horloge

Cette technologie supprime un certain pourcentage des signaux d'horloge pour l'unité centrale. Avec une limitation est de 25 %, une impulsion sur quatre est omise. À 87,5 %, seule une impulsion sur huit atteint le processeur. Les économies d'énergie ne sont toutefois pas tout à fait linéaires. La limitation de la fréquence d'horloge n'est normalement utilisée que si le contrôle de la fréquence est indisponible ou si l'on veut optimiser les économies d'énergie. Elle doit être contrôlée par un processus spécial. L'interface système est `/proc/acpi/processor/*/throttling`.

Mise en veille du processeur

Lorsqu'il n'y a rien à faire, le système d'exploitation envoie au processeur une commande `halt`, qui le met en veille. Trois états sont possibles : C1, C2 et C3. Dans l'état le plus économe, C3, même la synchronisation du cache du processeur avec la mémoire principale est arrêtée. Cet état ne peut donc être appliqué que si aucun autre périphérique ne modifie le contenu de la mémoire principale via le bus principal. Certains pilotes empêchent l'utilisation de C3. L'état en cours est affiché dans `/proc/acpi/processor/*/power`.

La limitation de l'utilisation du processeur et le contrôle de la fréquence ne sont utiles que si le processeur est occupé. En effet, le mode C le plus économique est toujours appliqué lorsque le processeur est inactif. Si l'unité centrale est occupée, il est recommandé de recourir au contrôle de la fréquence pour économiser l'énergie : le processeur ne fonctionnant souvent qu'avec une charge partielle, il peut être utilisé avec une fréquence plus basse. La meilleure approche reste souvent le contrôle dynamique de la fréquence par un démon, par exemple powersaved. Un réglage statique sur une fréquence basse est utile lorsque l'ordinateur fonctionne sur la batterie, ou si vous voulez qu'il refroidisse ou qu'il ne fasse pas de bruit.

Ne limitez l'utilisation du processeur qu'en dernier ressort (par exemple, pour allonger la durée de fonctionnement de la batterie en cas de charge élevée du système). Certains systèmes ne fonctionnent pas de manière optimale lorsqu'ils sont trop limités. En outre, la limitation de l'unité centrale ne sert à rien si celle-ci est peu sollicitée.

Sous SUSE Linux, ces technologies sont contrôlées par le démon powersave, dont la configuration est décrite à la Section 21.5, « Paquetage powersave » (p. 297).

21.3.3 Outils ACPI

Il existe un grand nombre d'outils ACPI plus ou moins complets : certains permettent seulement d'afficher des informations, comme le niveau de charge de la batterie ou la température (acpi, klaptopdaemon, wmacpimon, etc.) ; d'autres facilitent l'accès aux structures dans `/proc/acpi` ou facilitent la surveillance des modifications (akpi, acpiw, gtkacpiw) ; d'autres, enfin, permettent de modifier les tables ACPI dans le BIOS (paquetage `pmtools`).

21.3.4 Dépannage

Il existe deux types de problèmes. Le code ACPI du kernel peut comporter des bogues qui n'ont pas été détectés à temps. Un correctif pourra alors être téléchargé. Toutefois, la plupart des problèmes viennent du BIOS. Des écarts par rapport à la norme ACPI sont parfois volontairement intégrés au BIOS pour éviter des erreurs lors de la mise en oeuvre d'ACPI sur d'autres systèmes d'exploitation communément utilisés. Les composants matériels qui comportent des erreurs sérieuses de mise en oeuvre ACPI sont répertoriés dans une liste noire qui empêche le kernel Linux d'utiliser ACPI pour ces composants.

Lorsqu'un problème survient, commencez par mettre le BIOS à jour. Si l'ordinateur ne démarre toujours pas, utilisez l'un des paramètres de démarrage suivants :

pci=noacpi
: Ne pas utiliser ACPI pour configurer les périphériques PCI.

acpi=oldboot
: Effectuer uniquement une configuration simple des ressources. N'utiliser ACPI pour aucune autre tâche.

acpi=off
Désactiver ACPI.

AVERTISSEMENT: Problèmes de démarrage sans ACPI

Certaines machines récentes (en particulier les systèmes SMP ou AMD64) ont besoin de la gestion ACPI pour configurer le matériel. Sur ces machines, la désactivation du système ACPI peut entraîner des problèmes.

Après le démarrage du système, lisez les messages de démarrage avec la commande `dmesg | grep -2i acpi` (ou tous les messages, ACPI n'étant pas forcément la cause du problème). Si une erreur survient pendant l'analyse d'une table ACPI, vous pouvez remplacer la table la plus importante (DSDT) par une version améliorée. La table DSDT à l'origine de l'erreur sera alors ignorée. La procédure à suivre est décrite à la Section 21.5.4, « Dépannage » (p. 303).

La configuration du kernel comprend un paramètre qui permet d'activer les messages de débogage ACPI. Si un kernel avec débogage ACPI est compilé et installé, les experts qui recherchent des erreurs recevront des informations détaillées.

En cas de problèmes de matériel ou de BIOS, il est conseillé de contacter les fabricants. Même s'ils ne proposent pas d'assistance Linux, ils doivent être informésdes problèmes. En effet, ils ne prendront ces problèmes au sérieux que s'ils réalisent qu'un certain nombre de leurs clients utilisent Linux.

Pour plus d'informations

Documentation complémentaire et aide sur ACPI :

- `http://www.cpqlinux.com/acpi-howto.html` (guide pratique ACPI détaillé, avec correctifs DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (FAQ ACPI @Intel)
- `http://acpi.sourceforge.net/` (projet ACPI4Linux à Sourceforge)
- `http://www.poupinou.org/acpi/` (correctifs DSDT par Bruno Ducrot)

21.4 Repos du disque dur

Linux permet de mettre l'ensemble du disque dur en veille, s'il n'est pas nécessaire, ou de l'utiliser dans un mode plus économe ou plus silencieux. Sur les portables modernes, l'utilisateur n'a pas besoin de mettre manuellement le disque dur en veille : celui-ci passe automatiquement dans un mode d'exploitation économique dès qu'il n'est pas nécessaire. Toutefois, pour optimiser les économies d'énergie, vous pouvez essayer certaines des méthodes suivantes. La plupart des fonctions peuvent être contrôlées via powersaved et le module de gestion de l'alimentation YaST, décrit plus en détail à la Section 21.6, « Module de gestion de l'alimentation YaST » (p. 306).

L'application hdparm vous permet de modifier différents paramètres du disque dur. L'option `-y` met instantanément le disque dur en attente. Le paramètre `-Y` le met en veille. `hdparm -S x` provoque le ralentissement du disque après une période d'inactivité. Remplacez *x* comme suit : `0` désactive ce mécanisme, provoquant l'exécution continue du disque dur. Les valeurs comprises entre `1` et `240` sont multipliées par 5 secondes. Les valeurs comprises entre `241` et `251` correspondent à 1 à 11 fois 30 minutes.

Vous pouvez contrôler les options internes d'économie d'énergie du disque dur à l'aide de l'option `-B`. Sélectionnez une valeur comprise entre `0` et `255` pour optimiser les économies ou le débit. Le résultat dépend du disque dur et est difficile à évaluer. Pour rendre un disque dur plus silencieux, utilisez l'option `-M`. Sélectionnez une valeur comprise entre `128` et `254` pour le rendre plus silencieux ou plus rapide.

Il n'est souvent pas facile de mettre votre disque dur en veille. Sous Linux, de nombreux processus écrivent sur le disque dur, ce qui le réveille. Il est donc essentiel de comprendre comment Linux gère les données qui doivent être écrites sur le disque dur. Toutes les données sont d'abord mises en mémoire tampon dans la RAM. Ce tampon est contrôlé par le démon de mise à jour du kernel (kupdated). Lorsque les données atteignent une limite d'âge ou que la mémoire tampon atteint un niveau de remplissage, le contenu de la mémoire tampon est transféré sur le disque dur. La taille de la mémoire tampon est dynamique ; elle dépend de la taille de la mémoire et de la charge du système. Par défaut, kupdated est défini sur des intervalles courts pour optimiser l'intégrité des données. Il contrôle la mémoire tampon toutes les 5 secondes et appelle le démon bdflush lorsque les données ont plus de 30 secondes ou que le niveau de remplissage de la mémoire tampon atteint 30 %. bdflush écrit alors les données sur le disque dur. Il peut aussi les écrire, indépendamment de kupdated, si, par exemple, le tampon est plein.

AVERTISSEMENT: Altération de l'intégrité des données

Le fait de modifier les paramètres du démon de mise à jour du kernel met l'intégrité des données en danger.

En dehors de ces processus, les systèmes de fichiers à journalisation (par exemple, ReiserFS et Ext3) écrivent leurs métadonnées indépendamment de bdflush, ce qui prévient également les ralentissements du disque dur. Pour éviter ce problème, une extension du kernel a été développée spécialement pour les périphériques mobiles. Reportez-vous à `/usr/src/linux/Documentation/laptop-mode.txt` pour plus d'informations.

Un autre facteur important réside dans le comportement des programmes actifs. Par exemple, les bons éditeurs effectuent régulièrement des sauvegardes en arrière-plan du fichier en cours de modification (et réveillent le disque dur). Il est possible de désactiver ce type de fonctionnalité, aux dépens de l'intégrité des données.

Dans ce cadre, le postfix du démon de courrier utilise la variable `POSTFIX_LAPTOP`. Si cette variable est définie sur `yes`, le postfix accède bien plus rarement au disque dur. Il est cependant inutile de la modifier si l'intervalle de kupdated a été augmenté.

21.5 Paquetage powersave

Le paquetage `powersave` est responsable de la fonction d'économie d'énergie utilisée par les ordinateurs portables lorsqu'ils fonctionnent sur batterie. Certaines de ses fonctions sont également utiles pour les stations de travail normales et les serveurs, par exemple la mise en veille, la mise en attente, la fonctionnalité ACPI et la mise en veille des disques durs IDE.

Ce paquetage regroupe toutes les fonctions de gestion d'énergie de votre ordinateur. Il prend en charge le matériel utilisant ACPI, APM, les disques durs IDE, ainsi que les technologies PowerNow! ou SpeedStep. Les fonctionnalités des paquetages `apmd`, `acpid`, `ospmd` et `cpufreqd` (désormais nommé `cpuspeed`) ont été consolidées au sein du paquetage`powersave`. Les démons de ces paquetages ne doivent pas être exécutés parallèlement au démon powersave.

Même si votre système ne comporte pas tous les éléments matériel énumérés ci-dessus, utilisez le démon powersave pour contrôler la fonction d'économie d'énergie. Dans la

mesure où ACPI et APM s'excluent mutuellement, un seul de ces systèmes peut être utilisé sur votre ordinateur. Le démon détecte automatiquement toute modification dans la configuration matérielle.

21.5.1 Configuration du paquetage powersave

La configuration de powersave est normalement répartie dans plusieurs fichiers :

/etc/sysconfig/powersave/common
Ce fichier contient des paramètres généraux pour le démon powersave. La quantité de messages de débogage dans `/var/log/messages` peut par exemple être accrue en augmentant la valeur de la variable `DEBUG`.

/etc/sysconfig/powersave/events
Le démon powersave a besoin de ce fichier pour traiter les événements système. Des actions externes ou des actions effectuées par le démon lui-même peuvent être affectées à un événement. Pour les actions externes, le démon tente de lancer un fichier exécutable dans `/usr/lib/powersave/scripts/`. Actions internes prédéfinies :

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

throttle réduit la vitesse du processeur par la valeur définie dans MAX_THROTTLING. Cette valeur dépend du modèle actuel. dethrottle règle le processeur sur des performances maximales. suspend_to_disk, suspend_to_ram et standby déclenchent l'événement système permettant de passer en veille. Ces trois actions sont généralement responsables du déclenchement de la mise en veille, mais elles doivent toujours être associées à des événements système spécifiques.

Le répertoire /usr/lib/powersave/scripts contient des scripts pour le traitement des événements.

notify
Notification d'un événement par l'intermédiaire de la console, de X window ou d'un signal acoustique.

screen_saver
Active l'économiseur d'écran.

switch_vt
Utile si l'écran est déplacé après une mise en veille ou une mise en attente.

wm_logout
Enregistre les paramètres et se déconnecte de GNOME, de KDE ou d'un autre gestionnaire de fenêtres.

wm_shutdown
Enregistre les paramètres GNOME ou KDE et arrête le système.

Si, par exemple, la variable EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk" est définie, les deux scripts ou actions sont traités dans l'ordre spécifié, dès que l'utilisateur transmet à powersave la commande de mise en veille mise en veille sur disque. Le démon exécute le script externe /usr/lib/powersave/scripts/prepare_suspend_to_disk. Quand ce script a été traité, le démon exécute l'action interne do_suspend_to_disk et bascule l'ordinateur en veille une fois que le script a déchargé les modules critiques et arrêté les services.

Les actions exécutées en cas de clic sur le bouton de mise en veille peuvent être modifiées dans EVENT_BUTTON_SLEEP="notify suspend_to_disk". Dans ce cas, l'utilisateur est informé de la mise en veille par le script externe

notify. L'événement EVENT_GLOBAL_SUSPEND2DISK est ensuite généré, entraînant l'exécution des actions mentionnées et l'activation d'une veille système sécurisée. Le script notify peut être personnalisé à l'aide de la variable NOTIFY_METHOD dans /etc/sysconfig/powersave/common.

/etc/sysconfig/powersave/cpufreq
Contient des variables pour optimiser les paramètres dynamiques de fréquence du processeur.

/etc/sysconfig/powersave/battery
Contient les limites de la batterie et d'autres réglages spécifiques à celle-ci.

/etc/sysconfig/powersave/sleep
Ce fichier sert à activer les modes de veille et à déterminer les modules critiques à décharger et les services à arrêter avant un événement de type mise en veille ou mise en attente. Lors de la reprise du système, ces modules sont rechargés et les services sont redémarrés. Vous pouvez même retarder le déclenchement de la mise en veille, par exemple pour enregistrer des fichiers. Les paramètres par défaut concernent principalement les modules USB et PCMCIA. Un échec de mise en veille ou de mise en attente est généralement lié à certains modules. Consultez Section 21.5.4, « Dépannage » (p. 303) pour de plus amples informations sur la façon d'identifier l'erreur.

/etc/sysconfig/powersave/thermal
Active le contrôle du refroidissement et des données thermiques. Des détails à ce sujet sont disponibles dans le fichier /usr/share/doc/packages/powersave/README.thermal.

/etc/sysconfig/powersave/scheme_*
Regroupe les différents modèles qui adaptent la consommation d'énergie à certains scénarios de déploiement. Un certain nombre de modèles préconfigurés peuvent être utilisés tels quels. Les modèles personnalisés peuvent être enregistrés ici.

21.5.2 Configuration d'APM et d'ACPI

Mise en veille et mise en attente

Par défaut, les modes de veille sont inactifs, car ils ne fonctionnent pas encore sur certains ordinateurs. Il existe trois modes de veille ACPI de base et deux modes de veille APM.

Mise en veille sur disque (ACPI S4, mise en veille APM)
: Enregistre tout le contenu de la mémoire sur le disque dur. L'ordinateur est entièrement éteint et ne consomme pas d'électricité.

Mise en veille en RAM (ACPI S3, mise en veille APM)
: Enregistre l'état de tous les périphériques en mémoire principale. Seule la mémoire principale continue à consommer de l'énergie.

Mise en attente (ACPI S1, mise en attente APM)
: Éteint certains périphériques (selon le fabricant).

Assurez-vous que les options par défaut ci-après sont définies dans le fichier `/etc/sysconfig/powersave/events` pour assurer le traitement efficace de la mise en veille, de la mise en attente et de la reprise (paramètres par défaut après l'installation de SUSE Linux).

```
EVENT_GLOBAL_SUSPEND2DISK=
  "prepare_suspend_to_disk do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
  "prepare_suspend_to_ram do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
  "prepare_standby do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
  "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
  "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
  "restore_after_standby"
```

États de batterie personnalisés

Dans le fichier `/etc/sysconfig/powersave/battery`, définissez trois niveaux de charge de batterie (en pourcentage) qui déclenchent des alertes système ou des actions spécifiques quand ils sont atteints.

```
BATTERY_WARNING=20
BATTERY_LOW=10
BATTERY_CRITICAL=5
```

Les actions ou les scripts à exécuter quand les niveaux de charge tombent sous les limites spécifiées sont définis dans le fichier de configuration /etc/sysconfig/powersave/events. Les actions standard des boutons peuvent être modifiées conformément à ce qui est décrit dans Section 21.5.1, « Configuration du paquetage powersave » (p. 298).

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Adaptation de la consommation électrique à diverses conditions

Le comportement du système peut être adapté au type d'alimentation électrique. La consommation d'énergie du système doit être réduite quand le système n'est pas branché à une prise de courant et qu'il fonctionne sur batterie. De même, les performances doivent automatiquement être supérieures dès que le système est alimenté par une prise électrique. La fréquence du processeur, la fonction d'économie d'énergie de l'interface IDE et un certain nombre d'autres paramètres peuvent être modifiés.

Les actions à exécuter selon que l'ordinateur est connecté ou non au réseau électrique sont définies dans /etc/sysconfig/powersave/events. Sélectionnez les modèles à utiliser dans /etc/sysconfig/powersave/common.

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

Les modèles sont stockés dans des fichiers sous /etc/sysconfig/powersave. Les noms de fichiers suivent le format scheme_name-of-the-scheme. L'exemple fait référence à deux modèles : scheme_performance et scheme_powersave. performance, powersave, presentation et acoustic sont préconfigurés. Les modèles existants peuvent être modifiés, créés, supprimés ou associés à différents états d'alimentation à l'aide du module de gestion de l'alimentation YaST, décrit dans Section 21.6, « Module de gestion de l'alimentation YaST » (p. 306).

21.5.3 Fonctions ACPI supplémentaires

Si vous utilisez ACPI, vous pouvez contrôler la réponse de votre système aux *boutons ACPI* (marche, veille, capot ouvert et capot fermé). Configurez l'exécution de ces actions dans `/etc/sysconfig/powersave/events`. Consultez ce fichier de configuration pour obtenir des explications sur les options individuelles.

EVENT_BUTTON_POWER="wm_shutdown"
En cas de pression sur le bouton marche/arrêt, le système réagit par la fermeture du gestionnaire de fenêtres concerné (KDE, GNOME, fvwm, etc.).

EVENT_BUTTON_SLEEP="suspend_to_disk"
En cas de pression sur le bouton de veille, le système passe en veille sur disque.

EVENT_BUTTON_LID_OPEN="ignore"
Rien ne se passe en cas d'ouverture du capot.

EVENT_BUTTON_LID_CLOSED="screen_saver"
En cas de fermeture du capot, l'économiseur d'écran est activé.

Une limitation des performances du processeur est possible si la charge du processeur n'excède pas une limite spécifiée pendant un temps donné. Spécifiez la limite de charge dans `PROCESSOR_IDLE_LIMIT` et le délai dans `CPU_IDLE_TIMEOUT`. Si la charge du processeur reste inférieure à la limite au-delà du délai indiqué, l'événement configuré dans `EVENT_PROCESSOR_IDLE` est activé. Si le processeur est à nouveau occupé, `EVENT_PROCESSOR_BUSY` est exécuté.

21.5.4 Dépannage

Tous les messages d'erreur et alertes sont consignés dans le fichier `/var/log/messages`. Si vous ne trouvez pas les informations requises, augmentez le niveau de commentaire des messages de powersave à l'aide de `DEBUG` dans le fichier `/etc/sysconfig/powersave/common`. Augmentez la valeur de la variable à `7` ou même à `15` et redémarrez le démon. Les messages d'erreur plus détaillés dans `/var/log/messages` doivent permettre d'identifier l'erreur. Les sections suivantes traitent des problèmes les plus courants avec powersave.

ACPI est activé avec prise en charge du matériel mais des fonctions sont indisponibles

Si vous rencontrez des difficultés avec ACPI, utilisez la commande `dmesg|grep -i acpi` pour rechercher la sortie de `dmesg` pour les messages spécifiques à ACPI. Une mise à jour du BIOS peut être requise pour résoudre le problème. Rendez-vous sur la page d'accueil du fabricant de votre ordinateur portable, recherchez une mise à jour du BIOS et installez-la. Renseignez vous auprès de votre fabricant sur la conformité aux dernières spécifications ACPI. Si les erreurs persistent après la mise à jour du BIOS, procédez comme suit pour remplacer la table DSDT défectueuse dans votre BIOS par une DSDT mise à jour.

1. Téléchargez la DSDT pour votre système sur `http://acpi.sourceforge.net/dsdt/tables`. Vérifiez si le fichier est décompressé et compilé, c'est-à-dire s'il porte l'extension `.aml` (langage machine ACPI). Si tel est le cas, passez à l'étape 3.

2. Si l'extension de fichier du tableau téléchargé est `.asl` (langage source ACPI), compilez-le avec iasl (paquetage `pmtools`). Saisissez la commande `iasl -sa file.asl`. La dernière version de iasl (compilateur ACPI Intel) est disponible à l'adresse `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3. Copiez le fichier `DSDT.aml` où vous le souhaitez (`/etc/DSDT.aml` est conseillé). Modifiez `/etc/sysconfig/kernel` et adaptez le chemin vers le fichier DSDT en conséquence. Démarrez `mkinitrd` (paquetage `mkinitrd`). Lorsque vous installez le kernel et que vous utilisez `mkinitrd` pour créer un fichier `initrd`, la DSDT modifiée est intégrée et chargée à l'amorçage du système.

Le contrôle de fréquence du processeur ne fonctionne pas

Consultez les sources du kernel (`kernel-source`) pour savoir si votre processeur est pris en charge. Un module de kernel ou une option de module spécifique peuvent être requis pour activer le contrôle de fréquence du processeur. Ces informations sont disponibles dans `/usr/src/linux/Documentation/cpu-freq/*`. Si une option de module ou un module spécifique est requis, configurez-le(la) dans le fichier

/etc/sysconfig/powersave/cpufreq à l'aide des variables CPUFREQD_MODULE et CPUFREQD_MODULE_OPTS.

La mise en veille et la mise en attente ne fonctionnent pas

Plusieurs problèmes liés au kernel peuvent empêcher l'utilisation de la mise en veille et de la mise en attente sur les systèmes ACPI.

- Actuellement, les systèmes avec plus de 1 Go de mémoire vive (RAM) ne prennent pas la mise en veille en charge.
- De même, les systèmes multiprocesseurs et ceux équipés d'un processeur P4 (avec hyperthreading) ne prenent pas la mise en veille en charge.

L'erreur peut également être due à la mise en œuvre d'une DSDT défectueuse (BIOS). Dans ce cas, installez une nouvelle DSDT.

Sur les systèmes ACPI et APM : quand le système tente de décharger des modules défectueux, le système s'arrête ou la mise en veille ne se déclenche pas. La même chose peut se produire si vous ne déchargez pas les modules ou si vous n'arrêtez pas les services empêchant le succès de la mise en veille. Dans les deux cas, essayez d'identifier le module défectueux qui a empêché la mise en veille. Les fichiers journaux générés par le démon powersave dans /var/log/sleep mode sont très utiles dans cette optique. Si l'ordinateur ne passe pas en veille, la cause se situe dans le dernier module déchargé. Manipulez les réglages suivants dans /etc/sysconfig/powersave/sleep pour décharger les modules problématiques avant la mise en veille ou en attente.

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

Si vous utilisez la mise en veille ou la mise en attente dans des environnements réseaux changeants ou avec des systèmes de fichiers montés à distance, tels que Samba et NIS, utilisez automounter pour les monter ou ajoutez les services correspondants, par exemple smbfs ou nfs, dans la variable mentionnée ci-dessus. Si une application accède à un système de fichier monté à distance avant une mise en veille ou en attente, le service ne peut pas être arrêté correctement et le système de fichier ne peut pas être démonté

convenablement. Après la reprise du système, le système de fichiers peut être corrompu et doit alors être remonté.

Powersave ne tient pas compte des limites de batterie avec ACPI

Avec ACPI, le système d'exploitation peut demander au BIOS d'envoyer un message quand le niveau de charge de la batterie tombe sous une certaine limite. L'avantage de cette méthode est d'éviter une surveillance permanente de l'état de la batterie, ce qui grèverait les performances globales de l'ordinateur. Cependant, il arrive que la notification ne se fasse pas quand la limite est dépassée, même quand le BIOS est supposé prendre en charge cette fonction. Si cela se produit sur votre système, réglez la variable `FORCE_BATTERY_POLLING` du fichier `/etc/sysconfig/powersave/battery` sur `yes` pour forcer la surveillance de la batterie.

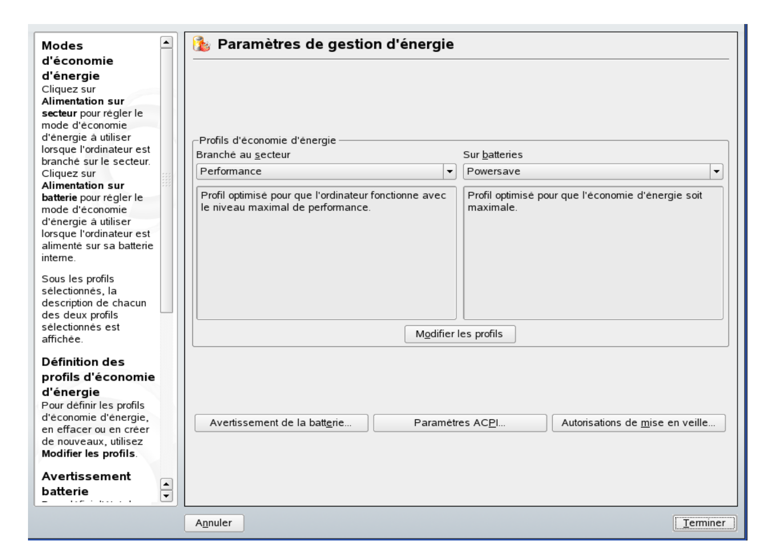
21.5.5 Pour plus d'informations

Des informations à propos du paquetage powersave sont également disponibles dans `/usr/share/doc/packages/powersave`.

21.6 Module de gestion de l'alimentation YaST

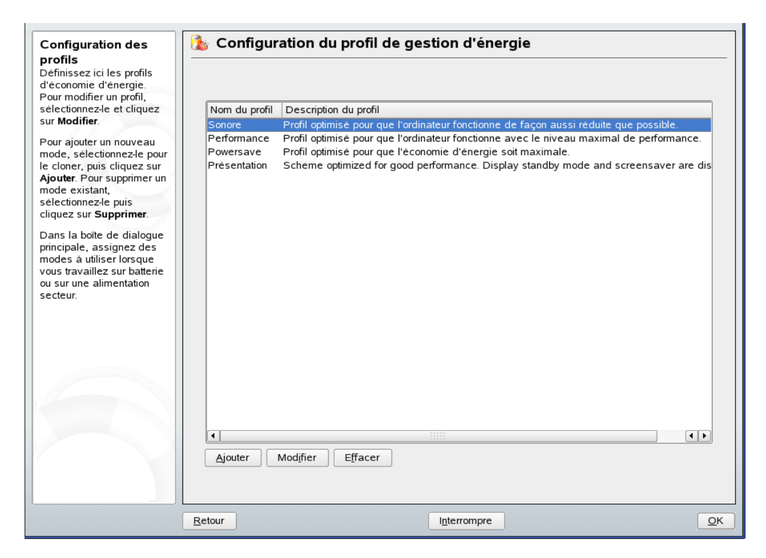
Le module de gestion de l'alimentation YaST permet de configurer tous les paramètres de gestion d'énergie déjà décrits. Démarrez ce module dans le centre de contrôle YaST avec *Système* → *Gestion de l'alimentation* pour accéder à la première boîte de dialogue. Il est présenté sur la Figure 21.1, « Sélection de modèle » (p. 307).

Figure 21.1 Sélection de modèle



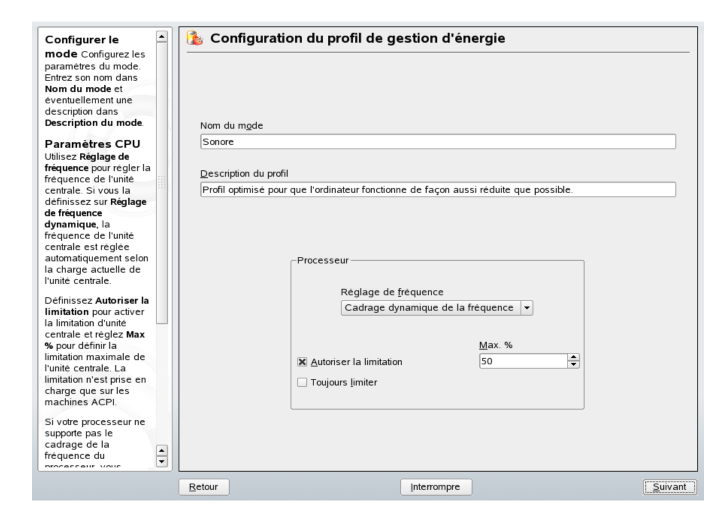
Cette boîte de dialogue permet de sélectionner les modèles à utiliser pour le fonctionnement en mode batterie et en mode secteur. Pour ajouter des modèles ou les modifier, cliquez sur *Modifier les profils*, ce qui vous permet d'accéder à un aperçu des modèles existants comme celui illustré dans Figure 21.2, « Aperçu des modèles existants » (p. 308).

Figure 21.2 Aperçu des modèles existants



Dans l'aperçu des modèles, sélectionnez celui que vous désirez modifier et cliquez sur *Modifier*. Pour créer un modèle, cliquez sur *Ajouter*. La boîte de dialogue qui s'ouvre est la même dans les deux cas. Elle est illustrée dans Figure 21.3, « Configuration d'un modèle » (p. 308).

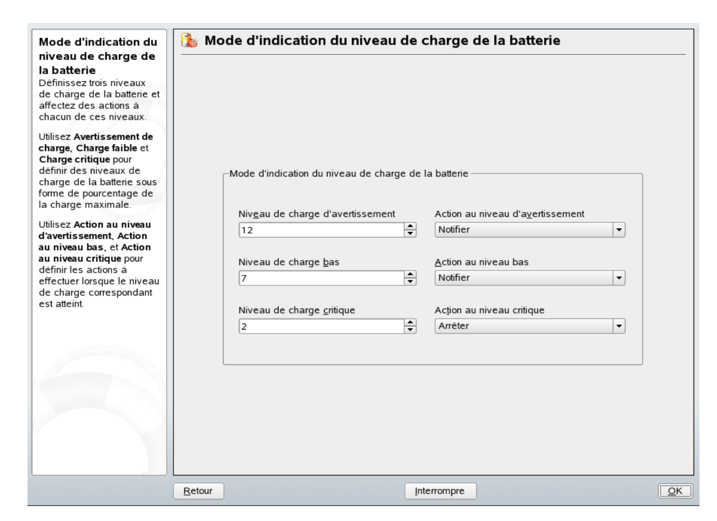
Figure 21.3 Configuration d'un modèle



Commencez par saisir un nom et une description pour le nouveau modèle ou le modèle modifié. Indiquez si les performances du processeur doivent être contrôlées pour ce modèle, et comment. Déterminez si l'adaptation et la limitation de fréquence doivent être utilisées et indiquez dans quelle mesure. Dans la boîte de dialogue suivante, relative au disque dur, définissez une *Règles du mode attente* permettant des performances maximum ou des économies d'énergie. *Règles sonores* contrôle le niveau sonore du disque dur (peu de disques prennent cette fonction en charge). *Règles de refroidissement* définit la méthode de refroidissement à employer. Ce type de contrôle thermique est malheureusement rarement pris en charge par le BIOS. Lisez `/usr/share/doc/packages/powersave/README.thermal` pour savoir comment exploiter le ventilateur et les méthodes de refroidissement passives.

Des paramètres généraux de gestion d'énergie peuvent également être définis dans la boîte de dialogue initiale via *Avertissement de la batterie*, *Paramètres ACPI* ou *Activer la mise en veille*. Cliquez sur *Avertissement de la batterie* pour accéder à la boîte de dialogue de contrôle de charge de la batterie, illustrée dans Figure 21.4, « Niveau de charge de la batterie » (p. 309).

Figure 21.4 *Niveau de charge de la batterie*

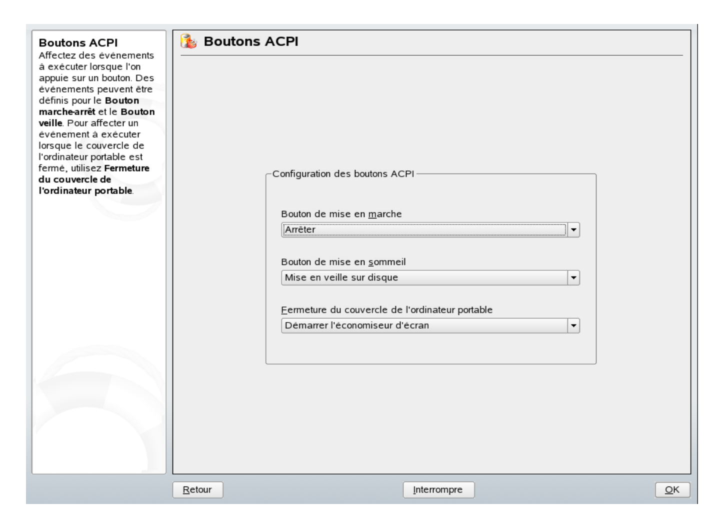


Le BIOS de votre système informe le système d'exploitation lorsque le niveau de charge tombe en deça de certaines limites configurables. Cette boîte de dialogue vous permet de définir trois limites : *Niveau de charge d'avertissement*, *Niveau de charge bas* et *Niveau de charge critique*. Des actions spécifiques sont déclenchées quand le niveau de charge passe sous ces limites. Les deux premiers niveaux déclenchent habituellement

une simple notification de l'utilisateur. Le troisième niveau, plus critique, entraîne la fermeture du système. En effet, l'énergie restante ne suffit plus à assurer son fonctionnement. Sélectionnez des niveaux de charge adaptés et les actions de votre choix, puis cliquez sur *OK* pour revenir à la boîte de dialogue initiale.



Figure 21.5 *Paramètres ACPI*



Cliquez sur *Paramètres ACPI* pour accéder à la boîte de dialogue de configuration des boutons ACPI. Il est présenté sur la Figure 21.5, « Paramètres ACPI » (p. 310). Les paramètres des boutons ACPI définissent comment le système doit réagir à certaines commutations. Configurez la réaction du système à la pression du bouton marche/arrêt ou veille et à la fermeture du capot du portable. Cliquez sur *OK* pour terminer la configuration et revenir à la boîte de dialogue initiale.

Cliquez sur *Activer la mise en veille* pour accéder à une boîte de dialogue dans laquelle vous pouvez déterminer si les utilisateurs peuvent utiliser les fonctions de mise en veille ou de mise en attente du système, et comment. Cliquez sur *OK* pour revenir à la boîte de dialogue initiale. Cliquez une nouvelle fois sur *OK* pour quitter ce module et valider vos paramètres de gestion d'énergie.

22 Communications sans fil

Diverses possibilités existent pour utiliser votre système Linux afin de communiquer avec d'autres ordinateurs, des téléphones mobiles ou des périphériques. WLAN (Wireless LAN) permet d'utiliser des ordinateurs portables. Bluetooth permet de connecter des composants systèmes (souris, clavier), des périphériques, des téléphones mobiles, des assistants personnels (PDA) et des ordinateurs individuels. IrDA est généralement utilisé pour la communication avec les PDA ou les téléphones mobiles. Ce chapitre présente ces trois technologies ainsi que leur configuration.

22.1 Réseau local sans fil

Les réseaux locaux sans fil ou WLAN (Wireless LAN) sont devenus un aspect incontournable de l'informatique mobile. À l'heure actuelle, la majorité des ordinateurs portables sont équipés d'une carte WLAN. Le standard 802.11, qui définit la communication sans fil des cartes WLAN, a été développé par l'IEEE. Ce standard assurait initialement un taux de transfert maximum de 2 Mbit/s, mais ses performances ont été considérablement améliorées. Les améliorations portent notamment sur la modulation, l'efficacité des transferts et le débit.

Tableau 22.1 *Aperçu de divers standards WLAN*

Nom	Fréquence (GHz)	Débit maximum (Mbit/s)	Remarque
802.11	2.4	2	Obsolète ; quasiment pas de périphériques disponibles
802.11b	2.4	11	Très répandu
802.11a	5	54	Moins courant
802.11g	2.4	54	Compatible avec 11b

Il existe en outre des standards propriétaires, comme la variante 802.11b de Texas Instruments (parfois appelée 802.11b+), qui affiche un débit maximum de 22 Mbit/s. Toutefois, les cartes employant ce standard sont peu répandues.

22.1.1 Matériel

SUSE Linux ne prend pas en charge les cartes 802.11 ; en revanche, il supporte la plupart des cartes 802.11a, 802.11b et 802.11g. Les nouvelles cartes sont généralement conformes au standard 802.11g, mais des cartes utilisant 802.11b sont toujours disponibles. Normalement, les cartes équipées des puces suivantes sont supportées :

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes

- Ralink RT2400, RT2500
- Texas Instruments ACX100, ACX111
- ZyDAS zd1201

Certaines cartes plus anciennes, rarement utilisées et retirées du commerce, sont également prises en charge. Une liste détaillée des cartes WLAN et des puces qu'elles utilisent est disponible sur le site Web de *AbsoluteValue Systems*, à l'adresse http://www.linux-wlan.org/docs/wlan_adapters.html.gz. La page http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz fournit également un aperçu des diverses puces WLAN.

Certaines cartes ont besoin d'une image de microprogramme qui doit être chargée lors de l'initialisation du pilote. C'est par exemple le cas des modèles Intersil PrismGT, Atmel, ainsi que TI ACX100 et ACX111. La fonction de mise à jour en ligne de YaST permet d'installer facilement le microprogramme. Le microprogramme des cartes Intel PRO/Wireless est fourni avec SUSE Linux et est automatiquement installé par YaST dès qu'une carte de ce type est détectée. Pour plus d'informations sur ce sujet, vous pouvez consulter le fichier `/usr/share/doc/packages/wireless-tools/README.firmware` installé sur votre système.

Il est possible d'utiliser les cartes dépourvues de prise en charge native de Linux, grâce à l'application ndiswrapper, qui utilise les pilotes Windows livrés avec la plupart des cartes WLAN. Vous trouverez une description de ndiswrapper sous `/usr/share/doc/packages/ndiswrapper/README.SUSE` si le paquetage `ndiswrapper` est installé. Pour plus d'informations sur ndiswrapper, consultez le site Web du projet à l'adresse http://ndiswrapper.sourceforge.net/support.html.

22.1.2 Fonction

Dans les réseaux sans fil, diverses techniques et configurations sont utilisées pour assurer des connexions rapides, fiables et sûres. Selon la configuration, différents types de fonctionnement sont appliqués. Il peut être difficile de choisir la bonne méthode d'authentification. Les méthodes de codage disponibles présentent toutes des avantages et des inconvénients.

Mode de fonctionnement

Fondamentalement, les réseaux sans fil peuvent être classés en réseaux gérés et en réseaux ad hoc. Les réseaux gérés possèdent un élément de gestion : le point d'accès. Dans ce mode (également appelé mode infrastructure), toutes les connexions des stations WLAN du réseau passent par le point d'accès, qui peut également fournir une connexion à un réseau Ethernet. Les réseaux ad hoc n'ont pas de point d'accès. Les stations communiquent directement entre elles. La portée et le nombre de stations des réseaux ad hoc sont très limités. C'est pourquoi un point d'accès est généralement plus efficace. Il est même possible d'utiliser une carte WLAN en guise de point d'accès. La plupart des cartes supportent cette fonctionnalité.

Les réseaux sans fil étant nettement plus faciles à infiltrer et à perturber que les réseaux filaires, les différents standards comprennent des méthodes d'authentification et de codage. Dans la version originale du standard IEEE 802.11, celles-ci sont rassemblées sous le terme WEP. Toutefois, WEP n'étant pas assez sûr (voir la section intitulée « Sécurité » (p. 320)), les acteurs du secteur du WLAN (réunis au sein de la *Wi-Fi Alliance*) ont défini une nouvelle extension nommée WPA, visant à corriger les défauts du protocole WEP. Le standard IEEE 802.11i (également appelé WPA2, parce que WPA est basé sur une pré-version de 802.11i) regroupe WPA et quelques autres méthodes d'authentification et de codage.

Authentification

Les réseaux gérés utilisent divers mécanimes d'authentification pour empêcher la connexion des stations non autorisées :

Ouvert
: Un système ouvert est un système ne nécessitant aucune authentification. N'importe quelle station de travail peut se connecter au réseau. Le codage WEP peut néanmoins être utilisé (voir la section intitulée « Chiffrement » (p. 316)).

Clé partagée (IEEE 802.11)
: Dans cette procédure, l'authentification utilise la clé WEP. Cette solution n'est cependant pas recommandée, car elle rend la clé WEP plus sensible aux attaques. Pour l'attaquant, il suffit d'épier assez longtemps la communication entre la station et le point d'accès : au cours de l'authentification, les deux parties s'envoient mutuellement les mêmes informations, une fois sous forme codée et une fois en clair. Il est donc possible de reconstruire la clé à l'aide d'outils adaptés. Cette

méthode, qui emploie la clé WEP pour l'authentification et le codage, n'améliore pas la sécurité du réseau. Une station qui possède la clé WEP appropriée peut authentifier, coder et décoder des données. Une station dépourvue de la bonne clé ne peut pas décrypter les paquets reçus. Par conséquent, elle ne peut pas communiquer, indépendamment de la nécessité de s'authentifier ou non.

WPA-PSK (IEEE 802.1x)

L'authentification WPA-PSK (PSK signifie "preshared key", c'est-à-dire clé prépartagée) fonctionne de façon similaire à l'authentification par clé partagée. Toutes les stations participantes, ainsi que le point d'accès, nécessitent la même clé. Cette clé, longue de 256 bits, est généralement saisie sous la forme d'une phrase d'authentification. Ce système, qui ne requiert pas de gestion de clé complexe comme celle de WPA-EAP, est mieux adapté à l'usage privé. C'est pourquoi WPA-PSK est parfois appelé WPA « Home ».

WPA-EAP (IEEE 802.1x)

WPA-EAP n'est pas un système d'authentification, mais un protocole de transport des informations d'authentification. Il est utilisé pour protéger les réseaux sans fil en entreprise, mais rarement utilisé dans les réseaux privés. WPA-EAP est parfois appelé WPA « Enterprise ».

WPA-EAP a besoin d'un serveur Radius pour authentifier les utilisateurs. EAP propose trois méthodes de connexion au serveur et d'authentification : TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) et PEAP (Protected Extensible Authentication Protocol). En quelques mots, ces options fonctionnent comme suit :

EAP-TLS

L'authentification TLS est basée sur l'échange mutuel de certificats, tant pour le serveur que pour le client. Tout d'abord, le serveur présente son certificat au client, qui l'évalue. Si le certificat est considéré comme valide, le client présente à son tour son certificat au serveur. TLS est sûr, mais nécessite une infrastructure de gestion des certificats au sein du réseau. Ce type d'infrastructure est rarement disponible dans les réseaux privés.

EAP-TTLS et PEAP

TTLS et PEAP sont des protocoles en deux étapes. Dans un premier temps, une connexion sécurisée est établie puis, dans un second temps, les données d'authentification client sont échangées. Avec ces protocoles, la gestion des certifications est nettement moins importante que dans TLS.

Chiffrement

Diverses méthodes de codage empêchent les personnes non autorisées de lire les paquets de données échangés dans un réseau sans fil et d'accéder au réseau :

WEP (défini dans IEEE 802.11)
: Ce standard utilise l'algorithme de codage RC4. Initialement de 40 bits, la clé a ensuite été ensuite étendue à 104 bits. La longueur est souvent définie comme égale à 64 bits ou 128 bits, si l'on inclut les 24 bits du vecteur d'initialisation. Ce standard présente néanmoins quelques points faibles. Les attaques dirigées contre les clés qu'il génère peuvent réussir. Cependant, il vaut mieux utiliser WEP qu'aucune méthode de codage du tout.

TKIP (défini dans WPA/IEEE 802.11i)
: Ce protocole de gestion de clé défini dans le standard WPA utilise le même algorithme de codage que WEP, mais corrige ses défauts. Une nouvelle clé étant générée pour chaque paquet de données, toute attaque dirigée contre ces clés sera vaine. TKIP est utilisé avec WPA-PSK.

CCMP (défini dans IEEE 802.11i)
: Le protocole CCMP décrit la gestion des clés. Généralement utilisé conjointement à WPA-EAP, il peut également être employé avec WPA-PSK. Le codage est effectué conformément au standard AES et est plus efficace que le codage RC4 du standard WEP.

22.1.3 Configuration avec YaST

Pour configurer votre carte réseau sans fil, démarrez le module *Carte réseau* de YaST. Dans *Configuration de l'adresse réseau*, sélectionnez le type de périphérique *Sans fil* et cliquez sur *Suivant*. La fenêtre *Configuration de la carte réseau sans fil*, illustrée dans Figure 22.1, « YaST : configuration de la carte réseau sans fil » (p. 317), vous permet d'effectuer les réglages de base pour votre carte WLAN :

Figure 22.1 *YaST : configuration de la carte réseau sans fil*

Mode de fonctionnement
Il existe trois modes d'intégration d'une station de travail à un réseau WLAN. Le mode le mieux adapté dépend du réseau employé : *Ad hoc* (réseau pair à pair sans point d'accès), *Géré* (réseau géré par un point d'accès) ou *Maître* (votre carte réseau sert de point d'accès). Avec l'authentification WPA-PSK ou WPA-EAP, le mode de fonctionnement sélectionné doit être *Géré*.

Nom du réseau (ESSID)
Toutes les stations d'un réseau local sans fil doivent avoir le même ESSID pour communiquer entre elles. Si vous ne spécifiez pas d'ESSID, la carte sélectionne automatiquement un point d'accès, qui n'est pas forcément celui que vous comptiez utiliser.

Mode d'authentification
Sélectionnez une méthode d'authentification adaptée à votre réseau : *Ouvert*, *Clé partagée*, *WPA-PSK* ou *WPA-EAP*. Si vous sélectionnez l'authentification WPA, un nom de réseau doit être défini.

Paramètres pour experts
Ce bouton ouvre une boîte de dialogue qui vous permet de procéder à la configuration approfondie de votre connexion WLAN. Cette boîte de dialogue est décrite en détail dans la suite.

Une fois les réglages de base effectués, votre station de travail est prête pour le déploiement dans le WLAN.

IMPORTANT: Sécurité dans les réseaux sans fil

Vous devez utiliser l'une des méthodes d'authentification et de codage supportées pour protéger le trafic sur votre réseau. Les connexions WLAN non codées permettent à des tiers d'intercepter toutes les données du réseau. Même un codage faible (WEP) vaut mieux que l'absence de protection. Pour plus d'informations, consultez la section intitulée « Chiffrement » (p. 316) et la section intitulée « Sécurité » (p. 320).

Selon la méthode d'authentification sélectionnée, YaST vous invitera peut-être à affiner vos réglages dans une autre boîte de dialogue. Pour *Ouvert*, aucune configuration n'est requise, puisque ce réglage ne supporte ni codage, ni authentification.

Clés WEP

Définissez le type de clé. Vous avez le choix entre *Phrase d'authentification (passphrase)*, *ASCII* et *Hexadécimal*. Vous pouvez conserver jusqu'à quatre clés différentes pour coder les données transmises. Cliquez sur *Clés multiples* pour accéder à la boîte de dialogue de configuration des clés. Définissez la longueur de la clé : *128 bits* ou *64 bits*. Le paramètre par défaut est *128 bits*. Dans la zone de liste située au bas de la boîte de dialogue, vous pouvez définir jusqu'à quatre clés différentes que votre station de travail utilisera pour le codage. Cliquez sur *Défini par défaut* pour définir l'une d'elles comme clé par défaut. Sans modification de votre part, YaST utilise la première clé saisie en guise de clé par défaut. Si la clé standard est supprimée, une des autres clés doit être sélectionnée manuellement comme clé par défaut. Cliquez sur *Modifier* pour modifier une entrée existante de la liste ou créer de nouvelles clés. Une fenêtre vous demande de sélectionner un type d'entrée (*Phrase d'authentification (passphrase)*, *ASCII* ou *Hexadécimal*). Si vous sélectionnez *Phrase d'authentification (passphrase)*, saisissez un mot ou une chaîne de caractères qui sera utilisé pour générer une clé de la longueur indiquée précédemment. *ASCII* demande la saisie de 5 caractères pour une clé 64 bits et de 13 caractères pour une clé 128 bits. Pour *Hexadécimal*, saisissez 10 caractères pour une clé 64 bits ou 26 caractères pour une clé 128 bits.

WPA-PSK

Pour saisir une clé pour WPA-PSK, sélectionnez la méthode d'entrée *Phrase d'authentification (passphrase)* ou *Hexadécimal*. En mode *Phrase d'authentification*

(passphrase), la saisie doit être comprise entre 8 et 63 caractères. En mode *Hexadécimal*, saisissez 64 caractères.

WPA-EAP
Saisissez les informations d'identification qui vous ont été communiquées par votre administrateur réseau. Pour TLS, fournissez le *Certificat du client* et le *Certificat du serveur*. TTLS et PEAP nécessitent une *Identité* et un *Mot de passe*. Le *Certificat du serveur* est facultatif. YaST recherche tous les certificats dans `/etc/cert`. Enregistrez les certificats reçus à cet emplacement et restreignez l'accès à ces fichiers à `0600` (lecture et écriture par le propriétaire).

Cliquez sur *Paramètres pour experts* pour quitter la boîte de dialogue de configuration de base de la connexion WLAN et accéder à la configuration pour experts. Cette boîte de dialogue propose les options suivantes :

Canal
La spécification d'un canal sur lequel la station WLAN doit travailler est uniquement nécessaire en modes *Ad hoc* et *Maître*. En mode *Géré*, la carte recherche automatiquement les canaux disponibles pour les points d'accès. En mode *Ad hoc*, sélectionnez l'un des 12 canaux proposés. Votre station utilisera ce canal pour communiquer avec les autres stations. En mode *Maître*, déterminez sur quel canal votre carte doit fonctionner comme point d'accès. Par défaut, cette option est réglée sur *Automatique*.

Débit binaire
Selon les performances du réseau, vous pouvez définir un débit pour les transmissions d'un point à un autre. Avec le réglage par défaut *Automatique*, le système essaye d'utiliser le débit maximum pour la transmission de données. Certaines cartes WLAN ne supportent pas la définition de débits binaires.

Point d'accès
Si votre environnement qui comporte plusieurs points d'accès, vous pouvez présélectionner l'un d'eux en spécifiant son adresse MAC.

Utiliser la gestion de l'énergie
Lorsque vous êtes en déplacement, utilisez les technologies d'économie d'énergie pour optimiser l'autonomie de votre batterie. Pour plus d'informations sur la gestion d'énergie, consultez Chapitre 21, *Gestion de l'alimentation* (p. 285).

22.1.4 Utilitaires

L'utilitaire hostap (paquetage `hostap`) permet d'utiliser une carte WLAN comme point d'accès. Vous trouverez de plus amples informations à propos de ce paquetage sur la page d'accueil du projet (http://hostap.epitest.fi/).

kismet (paquetage `kismet`) est un outil de diagnostic réseau qui permet d'écouter le trafic de paquets sur le réseau WLAN. Ainsi, il vous permet également de déceler les éventuelles tentatives d'intrusion dans votre réseau. De plus amples informations sont disponibles sur http://www.kismetwireless.net/ et dans la page d'aide.

22.1.5 Conseils et astuces pour la configuration d'un WLAN

Ces conseils peuvent vous aider à optimiser les performances, la stabilité et la sécurité de votre réseau WLAN.

Débit et stabilité

Les performances et la fiabilité d'un réseau sans fil dépendent avant tout de la qualité du signal échangé entre les stations de travail qui le composent. Des obstacles comme les murs affaiblissent considérablement le signal. Plus la qualité du signal est faible, plus la transmission est lente. Pendant le travail, vérifiez la qualité du signal en lançant iwconfig sur la ligne de commande (champ `Link Quality`) ou avec KInternet dans KDE. Si vous rencontrez des problèmes de qualité du signal, changez l'agencement de vos périphériques ou réglez la position des antennes de vos points d'accès. Pour un certain nombre de cartes WLAN PCMCIA, il est possible d'acheter des antennes auxiliaires, qui améliorent nettement la réception. Le débit indiqué par le fabricant, par exemple 54 Mbit/s, est une valeur nominale qui correspond à un maximum théorique. Dans la pratique, le débit maximum de données ne dépasse pas la moitié de cette valeur.

Sécurité

Si vous voulez configurer un réseau sans fil, n'oubliez pas que toute personne se trouvant dans la zone de transmission peut facilement y accéder si aucune mesure de sécurité n'est mise en œuvre. Vous devez donc activer une méthode de codage. Tous les points

d'accès et cartes WLAN prennent en charge le codage WEP. Bien que celui-ci ne soit pas parfaitement sûr, il constitue un obstacle pour les attaquants. WEP est généralement adapté à un usage privé. L'authentification WPA-PSK est plus efficace, mais elle ne fonctionne pas sur les points d'accès ni les routeurs anciens avec fonctionnalité WLAN. Sur certains périphériques, il est possible de mettre en oeuvre WPA grâce à une mise à jour du microprogramme. Par ailleurs, Linux ne supporte WPA que sur certains composants matériels. Au moment où nous rédigeons le présent document, WPA fonctionne uniquement avec les cartes utilisant des puces Atheros, Intel PRO/Wireless ou Prism2/2.5/3. Pour Prism2/2.5/3, WPA fonctionne uniquement avec le pilote hostap (voir la section intitulée « Problèmes avec les cartes Prism2 » (p. 321)). Si WPA n'est pas disponible, il vaut mieux utiliser WEP qu'aucun codage du tout. Dans les entreprises ayant des exigences de sécurité plus fortes, les réseaux sans fil doivent systématiquement utiliser WPA.

22.1.6 Dépannage

Si votre carte WLAN ne répond pas, vérifiez que vous avez téléchargé le microprogramme requis. Voir la Section 22.1.1, « Matériel » (p. 312). Les paragraphes qui suivent présentent un certain nombre de problèmes connus.

Périphériques réseau multiples

Les portables modernes possèdent généralement une carte réseau et une carte WLAN. Si vous avez configuré les deux périphériques avec DHCP (assignation automatique des adresses), vous risquez de rencontrer des problèmes de résolution de nom et de passerelle par défaut. Cette situation se caractérise par le fait qu'un ping vers le routeur fonctionne, mais que la navigation sur Internet est impossible. La base de données de support comporte un article à ce sujet, à l'adresse `http://portal.suse.com`. Pour trouver cet article, tapez « DHCP » dans la boîte de dialogue de recherche.

Problèmes avec les cartes Prism2

Plusieurs pilotes sont disponibles pour les périphériques dotés de puces Prism2. Chacune des cartes fonctionne plus ou moins bien avec les différents pilotes. L'utilisation de WPA avec ces cartes est soumise à l'emploi du pilote hostap. Si une carte de ce type fonctionne mal ou pas du tout, ou que vous voulez utiliser WPA, lisez le document `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

La prise en charge de WPA dans SUSE Linux est relativement récente et est encore en cours de développement. YaST ne supporte pas la configuration de toutes les méthodes d'authentification WPA. Tous les pilotes et cartes WLAN ne supportent pas WPA. Sur certaines cartes, une mise à jour du microprogramme est nécessaire pour assurer la prise en charge de WPA. Si vous voulez utiliser WPA, lisez `/usr/share/doc/packages/wireless-tools/README.wpa`.

22.1.7 Pour plus d'informations

Le site Internet de Jean Tourrilhes, qui a développé les outils "*Wireless Tools*" pour Linux, est une mine d'informations utiles à propos des réseaux sans fil. Voir `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`.

22.2 Bluetooth

La technologie sans fil Bluetooth sert à connecter entre eux plusieurs périphériques (téléphones cellulaires, agendas personnels, dispositifs périphériques, ordinateurs portables) ou des composants système (clavier ou souris). Son nom vient du roi danois Harald Blaatand, surnommé « Harald la Dent bleue » (Bluetooth), qui a unifié en un seul royaume plusieurs factions ennemies de Scandinavie. Le logo Bluetooth est composé des runes correspondant aux initiales « H » (sorte d'étoile) et « B ».

La technologie Bluetooth se différencie sur plusieurs points importants de la technologie IrDA. Premièrement, les périphériques n'ont pas besoin de « se voir » les uns les autres directement et, deuxièmement, il possible de connecter plusieurs périphériques en réseau. Toutefois, le taux de transfert de données est au maximum de 720 Kbits/s (version 1.2 actuelle). En théorie, avec la technologie Bluetooth, il est même possible de communiquer à travers des murs. En pratique, cependant, cela dépend des propriétés du mur et de la classe de périphériques. Il existe trois classes de périphériques avec des portées de transmission allant de dix à cent mètres.

22.2.1 Basiques

Les sections suivantes soulignent les principes de base du fonctionnement de la technologie Bluetooth. Vous obtiendrez des renseignements sur les configurations logicielles requises, sur l'interaction entre Bluetooth et votre système, ainsi que sur le fonctionnement des profils Bluetooth.

Logiciel

Pour pouvoir utiliser la technologie Bluetooth, vous avez besoin d'un adaptateur Bluetooth (intégré ou externe), de pilotes et d'une pile de protocoles Bluetooth. Le noyau Linux contient déjà les pilotes de base pour utiliser Bluetooth. Le système Bluez est utilisé comme pile de protocoles. Pour garantir le fonctionnement des applications avec Bluetooth, vous devez installer les paquetages de base `bluez-libs` et `bluez-utils`. Ces paquetages fournissent des services et des utilitaires requis. De plus, certains adaptateurs (Broadcom ou AVM BlueFritz!, par exemple) requièrent l'installation du paquetage `bluez-firmware`. Le paquetage `bluez-cups` permet d'imprimer via des connexions Bluetooth.

Interaction générale

Un système Bluetooth se compose de quatre couches interdépendantes qui fournissent les fonctionnalités voulues :

Matériel
L'adaptateur et un pilote approprié pour une prise en charge par le noyau Linux.

Fichiers de configuration
Pour contrôler le système Bluetooth.

Démons
Services contrôlés par les fichiers de configuration qui fournissent des fonctionnalités.

Applications
Les applications permettent à l'utilisateur d'utiliser et de contrôler les fonctionnalités fournies par les démons.

Lorsque vous insérez un adaptateur Bluetooth, son pilote est chargé par le système d'enfichage à chaud. Une fois le pilote chargé, le système recherche dans les fichiers

de configuration des informations pour déterminer si le système Bluetooth doit être démarré. Si tel est le cas, il détermine les services à lancer. En fonction de ces informations, les démons correspondants sont lancés. Les adaptateurs Bluetooth sont examinés pendant leur installation. Si au moins un adaptateur est détecté, le système Bluetooth est activé. Sinon, le système Bluetooth est désactivé. Si vous ajoutez ultérieurement un périphérique Bluetooth, vous devez l'activer manuellement.

Profils

Avec la technologie Bluetooth, les services sont définis au moyen de profils (par exemple, le profil de transfert de fichiers, le profil d'impression de base et le profil de réseau personnel). Pour permettre à un périphérique d'utiliser les services d'un autre périphérique, ils doivent tous les deux comprendre le même profil. Or, cette information est souvent omise dans le paquetage et le manuel du périphérique. Malheureusement, certains fabricants ne respectent pas strictement les définitions de chaque profil. Malgré tout, la communication entre les périphériques fonctionne généralement sans problèmes.

Dans le texte suivant, les périphériques locaux sont ceux reliés physiquement à l'ordinateur. Tous les autres périphériques qui ne sont accessibles que via des connexions sans fil sont appelés périphériques distants.

22.2.2 Configuration

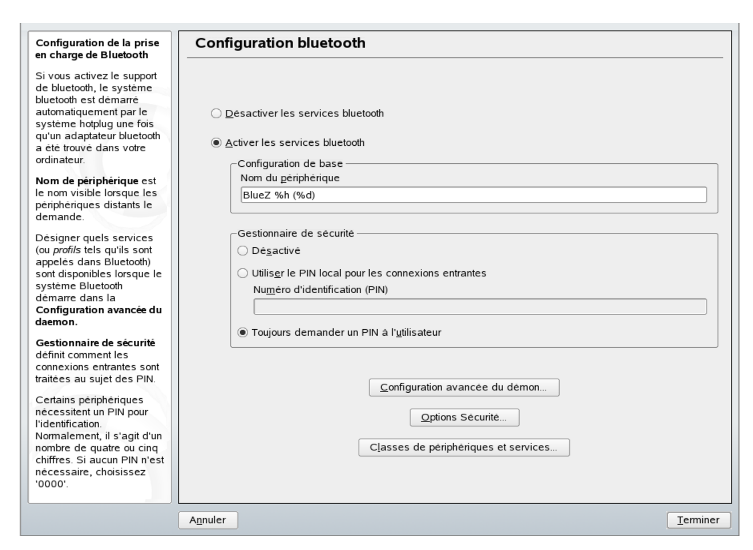
Cette section sert d'introduction à la configuration Bluetooth. Vous apprendrez quels fichiers de configuration entrent en jeu, quels outils sont nécessaires et comment configurer Bluetooth avec YaST ou manuellement.

Configuration de la technologie Bluetooth avec YaST

Pour configurer la prise en charge de Bluetooth sur votre système, utilisez le module YaST Bluetooth, illustré à la Figure 22.2, « Configuration YaST Bluetooth » (p. 325). Dès que le système d'enfichage à chaud détecte un adaptateur Bluetooth sur votre système (par exemple, pendant le démarrage ou lorsque vous branchez un adaptateur), Bluetooth est automatiquement lancé selon les paramètres configurés dans ce module.



***Figure 22.2** Configuration YaST Bluetooth*



À la première étape de la configuration, déterminez si les services Bluetooth doivent être lancés sur votre système. Si vous avez activé les services Bluetooth, vous pouvez configurer deux éléments. Premièrement, le *Nom du périphérique*. Il s'agit du nom affiché par les autres périphériques une fois que votre ordinateur a été détecté. Il existe deux variables d'emplacement : `%h`, qui remplace le nom d'hôte du système (pratique, par exemple, s'il est assigné de manière dynamique par DHCP), et `%d`, qui insère le numéro d'interface (utile uniquement si plusieurs adaptateurs Bluetooth sont installés sur votre ordinateur). Par exemple, si vous entrez `Laptop %h` dans le champ et si DHCP assigne le nom `unit123` à votre ordinateur, les autres périphériques distants vont identifier votre ordinateur comme `Laptop unit123`.

Le paramètre *Gestionnaire de sécurité* est lié au comportement du système local lorsqu'un périphérique distant tente de se connecter. La différence se situe au niveau de la gestion du code PIN (Personal Identification Number - numéro d'identification personnelle). Soit vous autorisez tout périphérique à se connecter sans code PIN, soit vous déterminez comment choisir le code PIN approprié si ce numéro est requis. Vous pouvez entrer un code PIN (enregistré dans un fichier de configuration) dans le champ de saisie approprié. Si un périphérique tente de se connecter, il commence par utiliser ce code PIN. S'il échoue, il change de comportement et n'utilise plus de code PIN. Pour une sécurité maximale, la meilleure option est *Toujours demander un PIN à l'utilisateur*. Cette option permet d'utiliser différents codes PIN pour différents périphériques (distants).

Cliquez sur *Configuration avancée du démon* pour ouvrir la boîte de dialogue dans laquelle vous sélectionnez et configurez les services disponibles (appelés *profils* dans Bluetooth). Tous les services disponibles s'affichent dans une liste. Vous pouvez les activer ou les désactiver en cliquant sur *Activer* ou *Désactiver*. Cliquez sur *Modifier* pour ouvrir la boîte de dialogue dans laquelle vous indiquez des arguments supplémentaires pour le service sélectionné (démon). N'effectuez des modifications que si vous êtes familiarisé avec ce service. Une fois les démons configurés, cliquez sur *OK* pour quitter cette boîte de dialogue.

De retour dans la boîte de dialogue principale, cliquez sur *Options Sécurité* pour ouvrir la boîte de dialogue de la sécurité. Indiquez les paramètres de chiffrement, d'authentification et d'analyse. Quittez la boîte de dialogue de la sécurité pour revenir à la boîte de dialogue principale. Cliquez sur *Terminer* pour fermer la boîte de dialogue principale. Votre système Bluetooth est alors prêt.

Dans la boîte de dialogue principale, vous pouvez également accéder à la boîte de dialogue *Classes de périphériques et services*. Les périphériques Bluetooth sont regroupés en différentes classes de périphériques. Dans cette boîte de dialogue, choisissez la classe appropriée pour votre ordinateur (*Bureau* ou *Portable*, par exemple). La classe de périphérique n'est pas un élément très important, contrairement à la classe de service, que vous définissez également dans cette boîte de dialogue. Parfois, les périphériques Bluetooth distants, tels que les téléphones cellulaires, n'autorisent que certaines fonctions s'ils peuvent détecter la classe de service appropriée définie sur votre système. C'est souvent le cas des téléphones cellulaires qui attendent une classe intitulée *Transfert d'objet* pour autoriser le transfert des fichiers depuis ou à partir de l'ordinateur. Vous pouvez choisir plusieurs classes. Il n'est pas utile de sélectionner tous les classes « juste au cas où ». La sélection par défaut doit convenir à la plupart des cas.

Pour utiliser Bluetooth pour configurer un réseau, activez *PAND* dans le boîte de dialogue *Configuration avancée du démon* et définissez le mode du démon à l'aide du menu *Modifier*. Pour une connexion réseau Bluetooth fonctionnelle, un démon de réseau personnel doit fonctionner en mode *Écoute* et son homologue en mode *Recherche*. Par défaut, le mode *Écoute* est prédéfini. Adaptez le comportement de votre démon de réseau personnel. De plus, configurez l'interface `bnepX` (`X` est le numéro du périphérique au sein du système) dans le module *Carte réseau* de YaST.

Configuration manuelle du système Bluetooth

Les fichiers de configuration de chaque composant du système Bluez se trouvent dans le répertoire `/etc/bluetooth`. La seule exception est le fichier `/etc/sysconfig/bluetooth` servant au lancement des composants, qui est modifié par le module YaST.

Seul l'utilisateur `root` peut modifier les fichiers de configuration décrits ci-après. Actuellement, il n'existe pas d'interface graphique pour modifier tous les paramètres. Vous pouvez définir les principaux dans le module YaST Bluetooth, conformément à la section intitulée « Configuration de la technologie Bluetooth avec YaST » (p. 324). Tous les autres paramètres ne représentent un intérêt que pour les utilisateurs expérimentés, pour des cas particuliers. Les paramètres par défaut sont généralement suffisant.

Un code PIN fournit une protection de base contre les connexions indésirables. Les téléphones portables demandent généralement un code PIN lors de l'établissement du premier contact (ou lors de la configuration d'un contact de périphérique sur le téléphone). Pour que deux périphériques puissent communiquer entre eux, ils doivent s'identifier avec le même code PIN. Sur l'ordinateur, le code PIN se trouve dans le fichier `/etc/bluetooth/pin`.

IMPORTANT: Sécurité des connexions Bluetooth

Malgré les codes PIN, la transmission entre deux périphériques n'est pas toujours totalement sécurisée. Par défaut, l'authentification et le chiffrement des connexions Bluetooth sont désactivés. Si vous activez l'authentification et le chiffrement, cela peut générer des problèmes de communication avec certains périphériques Bluetooth.

Vous pouvez modifier plusieurs paramètres, tels que le nom des périphériques et le mode de sécurité, dans le fichier de configuration `/etc/bluetooth/hcid.conf`. Les paramètres par défaut sont généralement suffisant. Ce fichier contient des commentaires décrivant les options des différents paramètres.

Deux sections dans le fichier inclus sont intitulées `options` et `device`. La première contient des informations générales que hcid utilise pour le démarrage. La deuxième contient les paramètres de chaque périphérique Bluetooth local.

L'un des paramètres les plus importants de la section `options` est `security auto;` (sécurité automatique). Si sa valeur est `auto`, hcid tente d'utiliser le code PIN local pour les connexions entrantes. En cas d'échec, sa valeur devient `none` (aucun) et il

établit de toute façon la connexion. Pour une sécurité optimale, vous devez définir la valeur `user` (utilisateur) pour ce paramètre par défaut afin de garantir que le système demande à l'utilisateur d'entrer un code PIN chaque fois qu'il établit une connexion.

Définissez le nom sous lequel l'ordinateur s'affiche à l'autre extrémité, dans la section `device` (périphérique). Définissez dans cette section la classe de périphérique : `Desktop` (ordinateur de bureau), `Laptop` (ordinateur portable) ou `Server` (serveur). Vous pouvez également activer ou désactiver l'authentification et le chiffrement dans cette section.

22.2.3 Composants système et utilitaires

L'opérabilité de Bluetooth dépend de l'interaction de plusieurs services. Au moins deux démons d'arrière-plan sont requis : hcid (pour « host controller interface daemon » ou démon d'interface du contrôleur hôte), qui sert d'interface pour le périphérique Bluetooth et qui contrôle ce dernier, et sdpd (pour « service discovery protocol daemon » ou démon de protocole de détection des services), grâce auquel un périphérique peut rechercher les services rendus disponibles par l'hôte. S'ils ne sont pas activés automatiquement au démarrage du système, vous pouvez activer les deux démons hcid et sdpd à l'aide de la commande `rcbluetooth start`. Cette commande doit être exécutée par un utilisateur `root`.

Les paragraphes suivants décrivent brièvement les outils de shell les plus importants que vous pouvez utiliser pour travailler avec Bluetooth. Même si plusieurs composants graphiques sont maintenant disponibles pour contrôler Bluetooth, cela peut valoir la peine de s'intéresser à ces programmes.

Certaines de ces commandes ne peuvent être exécutées que par l'utilisateur `root`. Cela concerne notamment la commande `l2ping` *`adresse_du_périphérique`* qui permet de tester la connexion à un périphérique distant.

hcitool

Utilisez hcitool pour déterminer si les périphériques locaux et distants sont détectés. La commande `hcitool dev` permet d'établir la liste des périphériques locaux. Comme résultat, une ligne au format *`nom_de_l'interface adresse_du_périphérique`* est générée pour chaque périphérique local détecté.

Recherchez les périphériques distants à l'aide de la commande `hcitool inq`. Trois valeurs sont renvoyées pour chaque périphérique détecté : l'adresse du périphérique, le décalage d'horloge et la classe du périphérique. L'adresse du périphérique est importante, car les autres commandes s'en servent pour identifier le périphérique cible. Le décalage d'horloge sert principalement pour des opérations techniques. La classe indique le type de périphérique et le type de service en tant que valeur hexadécimale.

Vous pouvez utiliser la commande `hcitool name` *`adresse_du_périphérique`* pour déterminer le nom d'un périphérique distant. Dans le cas d'un ordinateur distant, la classe et le nom du périphérique correspondent aux informations du fichier `/etc/bluetooth/hcid.conf` correspondant. Les adresses de périphériques locaux génèrent un message d'erreur.

hciconfig

La commande `/usr/sbin/hciconfig` propose d'autres informations sur le périphérique local. Si vous exécutez `hciconfig` sans arguments, vous obtenez des informations sur le périphérique, telles que son nom (`hciX`), l'adresse du périphérique physique (nombre à 12 chiffres au format `00:12:34:56:78`), ainsi que des informations sur la quantité de données transmises.

La commande `hciconfig hci0 name` affiche le nom renvoyé par votre ordinateur lorsqu'il reçoit des requêtes depuis des périphériques distants. En plus d'effectuer des requêtes sur les paramètres d'un périphérique local, la commande `hciconfig` permet de modifier ces paramètres. Par exemple, `hciconfig hci0 name TEST` définit la valeur `TEST` pour le nom.

sdptool

Vous pouvez utiliser le programme sdptool pour vérifier quels services sont rendus disponibles par un périphérique spécifique. La commande `sdptool browse` *`adresse_du_périphérique`* renvoie tous les services d'un périphérique. Utilisez la commande `sdptool search` *`code_du_service`* pour rechercher un service spécifique. Cette commande recherche le service demandé sur tous les périphériques accessibles. Si l'un des périphériques propose ce service, le programme imprime le nom complet du service renvoyé par le périphérique avec une brève description. Utilisez la commande `sdptool` sans paramètres pour afficher la liste de tous les codes de service possibles.

22.2.4 Applications graphiques

Dans Konqueror, entrez l'adresse URL `bluetooth:/` pour afficher la liste des périphériques Bluetooth locaux et distants. Double-cliquez sur un périphérique pour afficher la présentation des services qu'il propose. Si vous placez le pointeur de la souris sur l'un des services spécifiés, la barre d'état du navigateur indique le profil utilisé pour ce service. Si vous cliquez sur un service, une boîte de dialogue s'ouvre, avec un message qui vous demande quelle opération effectuer : enregistrer, utiliser le service (il faut alors démarrer une application) ou annuler cette opération. Cochez la case correspondante si vous ne voulez plus que cette boîte de dialogue s'affiche, mais si vous voulez que l'opération sélectionnée soit systématiquement exécutée. Certains services ne bénéficient pas encore d'une prise en charge. Pour d'autres, il se peut qu'il faille installer des paquetages supplémentaires.

22.2.5 Exemples

Cette section propose deux exemples types des scénarios Bluetooth possibles. Le premier indique comment établir une connexion réseau entre deux hôtes via Bluetooth. Le second illustre une connexion entre un ordinateur et un téléphone portable.

Connexion réseau entre deux hôtes

Dans le premier exemple, une connexion réseau est établie entre les hôtes *H1* et *H2*. Ces deux hôtes ont les adresses de périphérique Bluetooth *badr1* et *badr2* (déterminées sur les deux hôtes avec la commande `hcitool dev`, conformément à la description ci-avant). Les hôtes doivent être identifiés avec les adresses IP `192.168.1.3` (*H1*) et `192.168.1.4` (*H2*).

La connexion Bluetooth est établie à l'aide du démon pand (pour « personal area networking daemon » ou démon de réseau personnel). Les commandes suivantes doivent être exécutées par l'utilisateur `root`. Cette description se concentre sur les opérations propres à Bluetooth et ne propose pas une explication détaillée de la commande de réseau `ip`.

Entrez `pand -s` pour lancer le démon pand sur l'hôte *H1*. Vous pouvez ensuite établir une connexion sur l'hôte *H2* à l'aide de `pand -c` *`badr1`*. Si vous entrez `ip link show` sur l'un des hôtes pour afficher la liste des interfaces réseau disponibles, vous obtenez des résultats qui doivent contenir une entrée comparable à celle ci-après :

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
 link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

À la place de `00:12:34:56:89:90`, la sortie doit contenir l'adresse du périphérique local *badr1* ou *badr2*. Maintenant, vous devez assigner une adresse IP à cette interface et activer cette dernière. Pour *H1*, vous pouvez exécuter ces opérations à l'aide des deux commandes suivantes :

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

Pour *H2* :

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Maintenant, vous pouvez accéder à *H1* depuis *H2* via l'adresse IP `192.168.1.3`. Utilisez la commande `ssh 192.168.1.4` pour accéder à *H2* depuis *H1*, en considérant que *H2* exécute un sshd, activé par défaut sous SUSE Linux. La commande `ssh 192.168.1.4` peut également être exécutée par un utilisateur normal.

Transfert de données depuis un téléphone portable vers un ordinateur

Ce second exemple montre comment transférer une photo prise avec un téléphone portable doté d'un appareil photo intégré vers un ordinateur (sans que des frais supplémentaires ne soient appliqués pour l'envoi d'un message multimédia). Même si la structure des menus peut varier d'un téléphone portable à l'autre, la procédure est généralement la même. Reportez-vous au manuel de votre téléphone, si nécessaire. Cet exemple décrit le transfert d'une photo depuis un téléphone portable Sony Ericsson vers un ordinateur portable. Le service Obex-Push doit être disponible sur l'ordinateur qui doit accorder des droits d'accès au téléphone portable. À la première étape, le service est rendu disponible sur l'ordinateur portable. Pour ce faire, utilisez le démon opd du paquetage `bluez-utils`. Lancez ce démon à l'aide de la commande suivante :

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Deux paramètres importants sont utilisés : `--sdp`, qui enregistre le service auprès de sdpd, et `--path /tmp`, qui indique au programme où enregistrer les données reçues (dans le cas présent, dans `/tmp`). Vous pouvez également indiquer un autre répertoire pour lequel vous disposez des droits d'écriture.

Maintenant, le téléphone portable doit « apprendre » à identifier l'ordinateur. Pour ce faire, ouvrez le menu *Connect (Connexion)* du téléphone et sélectionnez *Bluetooth*. Si nécessaire, cliquez sur *Turn On (Activer)* avant de sélectionner *My devices (Mes périphériques)*. Sélectionnez *New device (Nouveau périphérique)* et laissez votre téléphone rechercher l'ordinateur portable. S'il détecte un périphérique, il en affiche le nom à l'écran. Sélectionnez le périphérique associé à l'ordinateur portable. Si votre code PIN vous est demandé, entrez celui spécifié dans le fichier `/etc/bluetooth/pin`. Maintenant, votre téléphone reconnaît l'ordinateur portable et ils peuvent échanger des données. Quittez le menu en cours et accédez à celui des images. Sélectionnez l'image à transférer et appuyez sur *More (Autres)*. Dans le menu suivant, appuyez sur *Send (Envoyer)* pour sélectionner un mode de transmission. Sélectionnez *Via Bluetooth*. L'ordinateur portable doit s'afficher dans la liste des périphériques cibles. Sélectionnez l'ordinateur portable pour lancer la transmission. L'image est ensuite enregistrée dans le répertoire indiqué dans la commande `opd`. Procédez de la même manière pour transférer des pistes audio vers l'ordinateur portable.

22.2.6 Dépannage

Si vous rencontrez des difficultés pour établir une connexion, procédez comme suit. N'oubliez pas que l'erreur peut provenir d'une extrémité ou l'autre de la connexion, ou des deux. Si possible, exécutez de nouveau la procédure qui pose problème avec un autre périphérique Bluetooth pour vérifier que ce n'est pas le périphérique qui est défectueux.

Le périphérique local s'affiche-t-il dans la liste générée par la commande `hcitool dev` ?

Si le périphérique local ne s'affiche pas dans cette liste, hcid n'a pas été lancé ou le périphérique n'est pas reconnu en tant que périphérique Bluetooth. Plusieurs causes sont possibles. Il se peut que le périphérique soit défectueux ou que le pilote approprié soit absent. Les ordinateurs portables avec technologie Bluetooth intégrée sont souvent doté d'un interrupteur marche/arrêt pour les périphériques sans fil, tels que WLAN et Bluetooth. Reportez-vous au manuel de votre ordinateur portable pour vérifier s'il est doté d'un tel interrupteur. Redémarrez le système Bluetooth avec la commande `rcbluetooth restart` et vérifiez si des erreurs sont signalées dans `/var/log/messages`.

Votre adaptateur Bluetooth a-t-il besoin d'un fichier de microprogramme ?

Si oui, installez `bluez-bluefw` et redémarrez le système Bluetooth à l'aide de la commande `rcbluetooth restart`.

La commande `hcitool inq` renvoie-t-elle d'autres périphériques ?

Testez plusieurs fois cette commande. La connexion peut être perturbée par des interférences, car d'autres périphériques utilisent également la bande de fréquences Bluetooth.

Les codes PIN sont-ils identiques ?

Vérifiez si le code PIN de l'ordinateur (dans `/etc/bluetooth/pin`) est le même que celui du périphérique cible.

Le périphérique distant peut-il « voir » votre ordinateur ?

Tentez d'établir la connexion depuis le périphérique portable. Vérifiez si ce périphérique voit l'ordinateur.

Est-il possible d'établir une connexion réseau (reportez-vous à la section intitulée « Connexion réseau entre deux hôtes » (p. 330)) ?

Il se peut que la configuration décrite à la section intitulée « Connexion réseau entre deux hôtes » (p. 330) ne fonctionne pas, et ce pour plusieurs raisons. Par exemple, il se peut que l'un des deux ordinateurs ne prenne pas en charge le protocole ssh. Essayez la commande `ping 192.168.1.3` ou `ping 192.168.1.4`. Si cette opération fonctionne, vérifiez si sshd est actif. Autre problème possible : l'un des deux périphériques a déjà des paramètres réseau qui génèrent un conflit avec l'adresse `192.168.1.X` de l'exemple. Si tel est le cas, essayez avec d'autres adresses, telles que `10.123.1.2` et `10.123.1.3`.

L'ordinateur portable s'affiche-t-il en tant que périphérique cible (reportez-vous à la section intitulée « Transfert de données depuis un téléphone portable vers un ordinateur » (p. 331)) ? Le périphérique mobile reconnaît-il le service Obex-Push sur l'ordinateur portable ?

Dans *My devices (Mes périphériques)*, sélectionnez le périphérique correspondant et affichez la liste des *services*. Si Obex-Push ne s'affiche pas (même après la mise à jour de la liste), le problème vient d'opd sur l'ordinateur portable. opd est-il actif ? Disposez-vous de droits d'écriture sur le répertoire spécifié ?

Le scénario décrit à la section intitulée « Transfert de données depuis un téléphone portable vers un ordinateur » (p. 331) fonctionne-t-il de la manière inverse ?

Si le paquetage `obexftp` est installé, vous pouvez utiliser la commande `obexftp -b` *`adresse_du_périphérique`* `-B 10 -p` *`image`* sur certains périphériques. Des tests ont été menés sur plusieurs modèles Siemens et Sony Ericsson qui sont fonctionnels. Reportez-vous à la documentation indiquée dans `/usr/share/doc/packages/obexftp`.

22.2.7 Pour plus d'informations

Pour obtenir une présentation détaillée de différentes instructions pour utiliser et configurer Bluetooth, reportez-vous au site http://www.holtmann.org/linux/bluetooth/. Autres informations et instructions pratiques :

- Mode d'emploi officiel de la pile de protocoles Bluetooth intégrée au kernel : http://bluez.sourceforge.net/howto/index.html
- Connexion à un assistant personnel PalmOS : http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html

22.3 Transmission de données infrarouge

IrDA (Infrared Data Association) est un standard de communication sans fil utilisant les infrarouges. De nombreux ordinateurs portables sont aujourd'hui équipés d'un émetteur-récepteur compatible IrDA, permettant la communication avec d'autres périphériques, comme les imprimantes, les modems, les réseaux locaux ou d'autres portables. La vitesse de transfert varie entre 2 400 bps et 4 Mbps.

Il existe deux modes de fonctionnement IrDA. Le mode standard, SIR, accède au port infrarouge par le biais d'une interface série. Ce mode fonctionne sur quasiment tous les systèmes et est suffisant pour la plupart des besoins. Le mode FIR, plus rapide, nécessite un pilote spécial pour la puce IrDA. Par manque de pilotes appropriés, tous les types de puces ne sont pas pris en charge en mode FIR. Sélectionnez le mode IrDA souhaité dans le BIOS de votre ordinateur. Le BIOS indique également quelle interface série est utilisée en mode SIR.

Des informations sur IrDA sont disponibles sur le site de Werner Heuser à l'adresse http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html. Vous pouvez également consulter le site Web du projet Linux IrDA, à l'adresse http://irda.sourceforge.net/.

22.3.1 Logiciel

Les modules de kernel requis sont inclus dans le paquetage kernel. Le paquetage `irda` fournit les applications nécessaires à la prise en charge de l'interface infrarouge. La documentation est accessible sous `/usr/share/doc/packages/irda/README` après l'installation du paquetage.

22.3.2 Configuration

Le service système IrDA n'est pas démarré automatiquement à l'amorçage du système. Utilisez le module IrDA de YaST pour l'activer. Un seul paramètre peut être modifié dans ce module : l'interface série utilisée par le périphérique infrarouge. La fenêtre de test affiche deux sorties. L'une d'elles correspond à la sortie de la commande `irdadump`, qui consigne tous les paquets IrDA envoyés et reçus. Cette sortie doit comporter le nom de l'ordinateur ainsi que les noms de tous les périphériques infrarouges situés dans la plage de transmission. Un exemple de message de ce type est visible dans Section 22.3.4, « Dépannage » (p. 336). Tous les périphériques vers lesquels une connexion IrDA existe sont répertoriés dans la partie inférieure de la fenêtre.

Le service IrDA consomme une quantité non négligeable d'électricité. En effet, un paquet de détection est envoyé à intervalles de quelques secondes pour détecter les autres périphériques de ce type. Si vous travaillez en mode batterie, il convient donc de démarrer la fonction IrDA uniquement lorsque c'est nécessaire. Saisissez la commande `rcirda start` pour l'activer ou `rcirda stop` pour la désactiver. Tous les modules de kernel requis sont automatiquement chargés quand cette interface est activée.

Une configuration manuelle peut être effectuée dans le fichier `/etc/sysconfig/irda`. Ce fichier contient une seule variable, `IRDA_PORT`, qui détermine l'interface à utiliser en mode SIR.

22.3.3 Utilisation

Des données peuvent être envoyées vers le fichier de périphérique `/dev/irlpt0` pour être imprimées. Le fichier de périphérique `/dev/irlpt0` fonctionne exactement comme l'interface câblée `/dev/lp0` normale, si ce n'est que les données d'impression sont envoyées sans fil à l'aide de rayons infrarouges. Pour l'impression, vérifiez que

l'imprimante se trouve dans le champ visuel de l'interface infrarouge de l'ordinateur et que la prise en charge infrarouge est démarrée.

Une imprimante utilisée via l'interface infrarouge peut être configurée à l'aide du module d'imprimante de YaST. Étant donné qu'elle n'est pas détectée automatiquement, configurez-la manuellement en cliquant sur *Autre (non détecté)*. Dans la boîte de dialogue suivante, sélectionnez *Imprimante IrDA*. `irlpt0` est généralement la bonne connexion. Des informations détaillées sur l'utilisation d'imprimantes sous Linux sont disponibles dans Chapitre 31, *Fonctionnement de l'imprimante* (p. 509).

La communication avec d'autres hôtes et avec des téléphones mobiles ou d'autres périphériques similaires intervient via le fichier de périphérique `/dev/ircomm0`. Les téléphones mobiles Siemens S25 et Nokia 6210, par exemple, peuvent se connecter à Internet par le biais de l'interface infrarouge à l'aide de l'application wvdial. La synchronisation de données avec un périphérique Palm Pilot est également possible, à condition que le paramètre de périphérique de l'application correspondante ait été réglé sur `/dev/ircomm0`.

Si vous le souhaitez, vous pouvez ne prendre en compte que les périphériques prenant en charge l'imprimante ou les protocoles IrCOMM. Les périphériques prenant en charge le protocole IROBEX, comme le Palm Pilot 3Com, sont accessibles à l'aide d'applications spéciales, comme irobexpalm et irobexreceive. Consultez *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`) pour plus d'informations. Les protocoles pris en charge par le périphérique sont répertoriés entre crochets après le nom du périphérique dans la sortie de `irdadump`. La prise en charge du protocole IrLAN est encore en « cours de développement. »

22.3.4 Dépannage

Si des périphériques connectés au port infrarouge ne répondent pas, utilisez la commande `irdadump` (en tant que `root`) pour vérifier si l'autre périphérique est reconnu par l'ordinateur. Un résultat semblable à celui de l'Exemple 22.1, « Sortie de irdadump » (p. 337) apparaît normalement quand une imprimante Canon BJC-80 se trouve dans le champ visuel de l'ordinateur :

***Exemple 22.1** Sortie de irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                        hint=0500 [ PnP Computer ] (21)
```

Vérifiez la configuration de l'interface s'il n'y a pas de sortie ou si l'autre périphérique ne répond pas. Vérifiez que l'interface adéquate est utilisée. L'interface infrarouge se situe parfois dans `/dev/ttyS2` ou dans `/dev/ttyS3` et une interruption différente de l'IRQ 3 est parfois utilisée. Ces paramètres peuvent être vérifiés et modifiés dans le menu de configuration du BIOS de quasiment tous les ordinateurs portables.

Une simple caméra vidéo peut également servir à déterminer si la diode infrarouge s'allume. En effet, la plupart des caméras vidéo permettent de visualiser les infrarouges, invisibles pour l'œil humain.

Administration

Sécurité sous Linux 23

La mascarade et les pare-feux permettent de contrôler le trafic et l'échange des données. L'interpréteur de commandes sécurisé (secure shell, SSH) permet à l'utilisateur de se connecter à une machine distante par une liaison chiffrée. Le chiffrement des fichiers ou de partitions entières sécurise vos données lorsque des tiers ont accès à votre système. Outre ces instructions purement techniques, vous trouverez des informations sur différents aspects de la sécurité dans les réseaux Linux.

23.1 Masquage et pare-feux

Lorsque Linux est utilisé dans un environnement réseau, vous pouvez utiliser des fonctions de kernel qui permettent de manipuler les paquets réseau afin de maintenir une séparation entre les secteurs interne et externe du réseau. L'infrastructure Linux Netfilter permet d'établir un pare-feu efficace qui isole les différents réseaux. Vous pouvez contrôler avec précision les paquets autorisés à franchir une interface réseau à l'aide d'iptables, structure de table générique qui permet de définir des ensembles de règles. Vous pouvez définir assez facilement ce type de filtre de paquets à l'aide de SUSEfirewall2 et du module YaST correspondant.

23.1.1 Filtrage des paquets avec iptables

Les composants netfilter et iptables sont chargés de filtrer et de manipuler les paquets réseau et sont également chargés de la traduction des adresses réseau (NAT - Network Address Translation). Les critères de filtrage et toute action associée sont stockés dans des chaînes, qui doivent être mises en correspondance les unes après les autres par

chaque paquet réseau entrant. Les chaînes à mettre en correspondance sont stockées dans des tables. La commande `iptables` permet de modifier ces tables et ces ensembles de règles.

Le kernel Linux gère trois tables, chacune correspondant à une catégorie spécifique de fonctions du filtre de paquets :

filtre
: Cette table comprend la plupart des règles de filtrage puisqu'elle implémente le mécanisme de *filtrage des paquets* au sens le plus strict, qui détermine par exemple si les paquets sont admis (`ACCEPT`) ou rejetés (`DROP`).

nat
: Cette table définit toutes les modifications apportées aux adresses source et cible des paquets. Ces fonctions vous permettent également d'implémenter le *masquage*, qui correspond à un cas particulier de NAT utilisé pour relier un réseau privé à Internet.

mangle
: Les règles contenues dans cette table permettent de manipuler les valeurs stockées dans les en-têtes IP (telles que le type de service).

Figure 23.1 *iptables : les chemins possibles d'un paquet*

Ces tables contiennent plusieurs chaînes prédéfinies à mettre en correspondance avec les paquets :

PREROUTING
: Cette chaîne concerne les paquets entrants.

INPUT
: Cette chaîne concerne les paquets destinés aux processus internes du système.

FORWARD
: Cette chaîne concerne les paquets qui sont uniquement routés via le système.

OUTPUT
: Cette chaîne concerne les paquets provenant du système lui-même.

POSTROUTING
: Cette chaîne concerne tous les paquets sortants.

La Figure 23.1, « iptables : les chemins possibles d'un paquet » (p. 343) illustre les chemins que peut emprunter un paquet réseau sur un système donné. Pour plus de clarté, cette figure regroupe les tables en chaînes, mais en réalité, ces chaînes sont conservées dans les tables mêmes.

Dans le cas le plus simple, un paquet entrant destiné au système arrive sur l'interface `eth0`. Le paquet est d'abord transmis à la chaîne `PREROUTING` de la table `mangle`, puis à la chaîne `PREROUTING` de la table `nat`. L'étape suivante, concernant le routage du paquet, indique que la cible réelle du paquet est un processus du système. Après être passé par les chaînes `INPUT` des tables `mangle` et `filter`, le paquet atteint finalement sa cible, à condition que les règles de la table `filter` coïncident réellement.

23.1.2 Principes de base du masquage

Le masquage est la forme de traduction d'adresses réseau (NAT) propre à Linux. Il permet de relier un petit réseau local, où les hôtes utilisent des adresses IP de la plage privée (consultez la Section 38.1.2, « Masques réseau et routage » (p. 609)), à Internet (où des adresses IP officielles sont utilisées). Pour que les hôtes du réseau local soient en mesure de se connecter à Internet, leurs adresses privées sont converties en adresses officielles. Cette opération s'effectue sur le routeur, qui tient le rôle de passerelle entre le réseau local et Internet. Le principe sous-jacent est simple : Le routeur possède plusieurs interfaces réseau, généralement une carte réseau et une interface distincte d'accès à Internet. Tandis que cette dernière relie le routeur au monde extérieur, une ou plusieurs autres interfaces le relient aux hôtes du réseau local. Ces hôtes du réseau local

étant connectés à la carte réseau (eth0 par exemple) du routeur, ils peuvent envoyer tous les paquets non destinés au réseau local à leur routeur ou leur passerelle par défaut.

IMPORTANT: Utilisation du masque réseau approprié

Lorsque vous configurez votre réseau, vérifiez que l'adresse de diffusion et le masque réseau sont bien les mêmes pour tous les hôtes locaux. Si ce n'est pas le cas, les paquets ne peuvent pas être routés correctement.

Comme indiqué précédemment, lorsque l'un des hôtes du réseau local envoie un paquet destiné à une adresse Internet, il est orienté vers le routeur par défaut. Toutefois, le routeur doit être configuré pour pouvoir transmettre ces paquets. Pour des raisons de sécurité, SUSE Linux n'active pas cette fonction dans une installation par défaut. Pour l'activer, définissez la variable `IP_FORWARD` du fichier `/etc/sysconfig/sysctl` sur `IP_FORWARD=yes`.

L'hôte cible de la connexion peut voir votre routeur mais ne sait rien sur l'hôte de votre réseau interne d'où proviennent les paquets. C'est la raison pour laquelle cette technique porte le nom de masquage. En raison de la traduction d'adresses, le routeur est la première destination de tout paquet de réponses. Il doit identifier ces paquets entrants et traduire leurs adresses cible, pour que les paquets puissent être transmis à l'hôte approprié dans le réseau local.

Le routage du trafic entrant dépend de la table de masquage. Il n'est donc pas possible d'ouvrir une connexion depuis l'extérieur vers un hôte interne. Il n'y aurait pas d'entrée dans la table pour ce type de connexion. Une connexion établie possède ainsi un état particulier dans cette table, de manière à ce que cet élément ne puisse pas être utilisé par une autre connexion.

Par conséquent, vous risquez de rencontrer des problèmes avec certains protocoles d'application, tels que ICQ, cucme, IRC (DCC, CTCP) et FTP (en mode PORT). Netscape, le programme FTP standard et bien d'autres utilisent le mode PASV. Ce mode passif pose bien moins de problèmes en matière de filtrage de paquets et de masquage.

23.1.3 Principes de base du pare-feu

Le terme *pare-feu* est probablement le plus utilisé pour décrire un mécanisme qui fournit et gère une liaison entre deux réseaux tout en contrôlant les flux de données circulant entre eux. En réalité, le mécanisme décrit dans la présente section est un *filtre*

de paquets. Il régule le flux de données en fonction de certains critères, tels que les protocoles, les ports et les adresses IP. Vous pouvez ainsi bloquer les paquets qui, selon leur adresse, ne sont pas censés atteindre votre réseau. Pour autoriser l'accès public à votre serveur Web, par exemple, vous devez ouvrir explicitement le port correspondant. Toutefois, un filtre de paquets n'analyse pas le contenu des paquets dont l'adresse est légitime (comme ceux qui sont destinés à votre serveur Web). Par exemple, si des paquets entrants ont pour objectif de mettre en péril un programme CGI sur votre serveur Web, le filtre de paquets les laisse tout de même passer.

Il existe un mécanisme plus efficace, mais également plus complexe, qui associe plusieurs types de systèmes, comme l'interaction d'un filtre de paquets avec le proxy ou la passerelle applicative. Dans ce cas, le filtre de paquets rejette tous les paquets destinés aux ports désactivés. Seuls les paquets destinés à la passerelle applicative sont acceptés. Cette passerelle ou ce proxy prétend être le client réel du serveur. D'une certaine manière, ce type de proxy peut être considéré comme un hôte de masquage au niveau du protocole utilisé par l'application. Squid, qui est un serveur proxy HTTP, correspond à ce type de proxy. Pour utiliser Squid, le navigateur doit être configuré pour communiquer via le proxy. Les pages HTTP demandées sont remises depuis le cache du proxy et les pages introuvables dans le cache sont extraites d'Internet par le proxy. Autre exemple, la suite proxy de SUSE (`proxy-suite`) fournit un proxy pour le protocole FTP.

La section suivante est consacrée au filtre de paquets fourni avec SUSE Linux. Pour plus d'informations sur le filtrage de paquets et l'utilisation d'un pare-feu, consultez le Firewall HOWTO (Guide pratique) inclus dans le paquetage `howto`. Lisez-le à l'aide de la commande `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz` si ce paquetage est installé.

23.1.4 SUSEfirewall2

SUSEfirewall2 est un script qui lit l'ensemble de variables dans `/etc/sysconfig/SuSEfirewall2` pour générer un ensemble de règles iptables. Il détermine trois zones de sécurité, même si seules les deux premières sont prises en compte dans l'exemple de configuration suivant :

Zone externe

L'hôte doit se protéger du réseau externe puisqu'il n'a aucun moyen de savoir ce qui s'y passe. Généralement, ce réseau externe est Internet mais il peut s'agir d'un réseau non protégé, comme un réseau WLAN.

Zone interne

Il s'agit du réseau privé, généralement le réseau local. Si les hôtes de ce réseau utilisent des adresses IP de la plage privée (consultez la Section 38.1.2, « Masques réseau et routage » (p. 609)), activez la traduction d'adresses réseau (NAT) pour que les hôtes du réseau interne puissent accéder au réseau externe.

Zone démilitarisée (DMZ)

Les hôtes situés dans cette zone peuvent être joints depuis le réseau externe et le réseau interne mais ne peuvent pas accéder au réseau interne. Vous pouvez utiliser ce paramètre pour installer une ligne de défense supplémentaire devant le réseau interne, puisque les systèmes DMZ sont isolés de ce réseau.

iptables supprime tout type de trafic réseau non explicitement autorisé par l'ensemble de règles de filtrage. Par conséquent, chaque interface associée à un trafic entrant doit être placée dans l'une de ces trois zones. Définissez les services ou protocoles autorisés pour chacune des zones. L'ensemble de règles s'applique uniquement aux paquets provenant d'hôtes distants. Le pare-feu ne filtre pas les paquets générés localement.

Vous pouvez effectuer la configuration via YaST (consultez la section intitulée « Configuration avec YaST » (p. 347)). Vous pouvez également l'effectuer manuellement dans le fichier `/etc/sysconfig/SuSEfirewall2`, qui contient des commentaires détaillés. En outre, vous trouverez quelques exemples de scénario dans `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES`.

Configuration avec YaST

IMPORTANT: Configuration automatique du pare-feu

Une fois l'installation terminée, YaST démarre automatiquement un pare-feu sur toutes les interfaces configurées. Si un serveur est configuré et activé sur le système, YaST peut modifier la configuration de pare-feu générée automatiquement à l'aide des options *Ouvrir le pare-feu pour l'interface sélectionnée* ou *Ouvrir port dans pare-feu* dans les modules de configuration du serveur. Certaines boîtes de dialogue du module du serveur comportent un

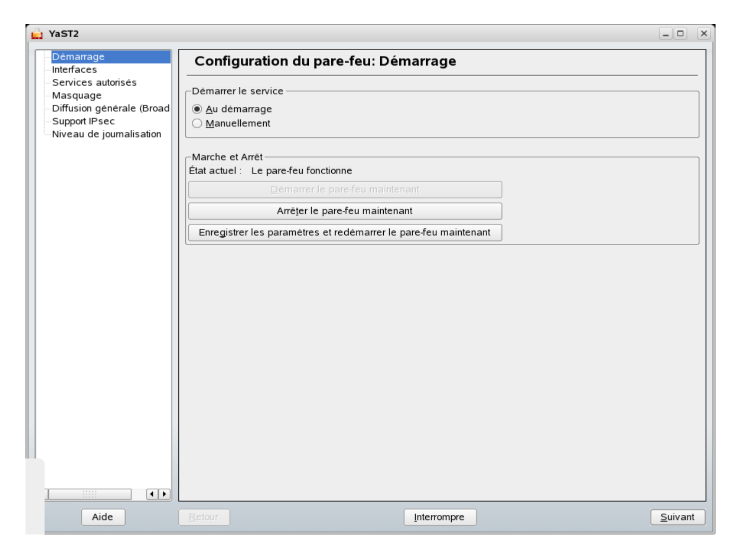
bouton *Détails du pare-feu* qui permet d'activer des ports et des services supplémentaires. Vous pouvez utiliser le module de configuration du pare-feu YaST pour activer, désactiver ou reconfigurer le pare-feu.

Pour la configuration graphique, vous pouvez accéder aux boîtes de dialogue YaST à partir du centre de contrôle YaST. Sélectionnez *Sécurité et Utilisateurs* → *Pare-feu*. La configuration est divisée en sept sections auxquelles vous accédez directement à partir de la structure de l'arborescence située à gauche.

Démarrage

Cette boîte de dialogue permet de définir le comportement au démarrage. Dans une installation par défaut, SUSEfirewall2 démarre automatiquement. Vous pouvez également démarrer et arrêter le pare-feu ici. Pour implémenter les nouveaux paramètres dans un pare-feu en cours d'exécution, utilisez *Enregistrer les paramètres et redémarrer le pare-feu maintenant*.

Figure 23.2 *Configuration YaST du pare-feu*



Interfaces

Toutes les interfaces réseau connues sont listées ici. Pour supprimer une interface d'une zone, sélectionnez-la, cliquez sur *Changer*, puis choisissez *Aucune zone assignée*. Pour ajouter une interface à une zone, sélectionnez-la, cliquez sur *Changer*, puis choisissez l'une des zones disponibles. Pour créer une interface spéciale avec vos propres paramètres, utilisez *Personnaliser*.

Services autorisés

Cette option vous permet d'offrir des services à partir de votre système à une zone vis-à-vis de laquelle il est protégé. Par défaut, le système est uniquement protégé des zones externes. Autorisez explicitement les services auxquels les hôtes externes doivent pouvoir accéder. Activez ces services après avoir sélectionné la zone souhaitée dans *Services autorisés pour la zone sélectionnée*.

Masquage

Le masquage vous permet de cacher votre réseau interne des réseaux externes, comme Internet. Il permet aussi aux hôtes du réseau interne d'accéder au réseau externe en toute transparence. Les requêtes du réseau externe vers le réseau interne sont bloquées alors que les requêtes du réseau interne semblent être émises par le serveur de masquage lorsqu'elles sont vues à l'extérieur. Si des services spéciaux d'une machine interne doivent être disponibles pour le réseau externe, ajoutez des règles spéciales de réacheminement pour le service correspondant.

Diffusion générale (Broadcast)

Cette boîte de dialogue vous permet de configurer les ports UDP qui permettent les diffusions. Ajoutez les numéros ou services de port nécessaires à la zone correspondante en les séparant par un espace. Consultez également le fichier `/etc/services`.

Cette boîte de dialogue permet également d'activer la journalisation des diffusions générales non autorisées. Cela risque d'être problématique car les hôtes Windows utilisent les diffusions générales pour obtenir des informations les uns sur les autres et génèrent donc de nombreux paquets non autorisés.

Support IPsec

Cette boîte de dialogue permet de déterminer si le service IPsec doit être disponible depuis le réseau externe. Déterminez les paquets de confiance sous *Détails*.

Niveau de journalisation

Il existe deux règles de journalisation : les paquets autorisés et les paquets non autorisés. Les paquets non autorisés sont ABANDONNÉS ou REJETÉS. Pour ces deux règles, sélectionnez *Tout journaliser*, *Ne journaliser que ce qui est critique* ou *Ne rien journaliser*.

Une fois la configuration du pare-feu terminée, cliquez sur *Suivant* pour quitter cette boîte de dialogue. Vous obtenez alors un résumé par zone de la configuration du pare-feu. Il vous permet de vérifier tous les paramètres. Ce résumé dresse la liste de tous les

services, ports et protocoles qui ont été autorisés. Pour modifier la configuration, cliquez sur *Retour*. Pour l'enregistrer, cliquez sur *Accepter*.

Configuration manuelle

Les paragraphes suivants fournissent des instructions détaillées pour une configuration réussie. Pour chaque élément de configuration, nous indiquons s'il concerne le pare-feu ou le masquage. Les aspects relatifs à la zone démilitarisée (DMZ) mentionnés dans le fichier de configuration ne sont pas abordés ici. En effet, ils s'appliquent uniquement à des infrastructures réseau plus complexes que l'on trouve dans les grandes sociétés (réseaux d'entreprise), qui nécessitent une configuration de grande envergure et des connaissances approfondies sur le sujet.

Activez d'abord SUSEfirewall2 pour votre niveau d'exécution (probablement 3 ou 5) à l'aide du module de YaST Services système (niveau d'exécution). Il crée les liens symboliques pour les scripts SUSEfirewall2_* dans les répertoires `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (pare-feu, masquage)
: Il s'agit du périphérique connecté à Internet. Pour une connexion par modem, saisissez `ppp0`. Pour une connexion RNIS, utilisez `ippp0`. Les connexions DSL utilisent `dsl0`. Indiquez `auto` pour utiliser l'interface qui correspond à la route par défaut.

`FW_DEV_INT` (pare-feu, masquage)
: Il s'agit du périphérique connecté au réseau interne privé (par exemple, `eth0`). Laissez ce champ vide s'il n'existe aucun réseau interne et si le pare-feu protège uniquement l'hôte sur lequel il est exécuté.

`FW_ROUTE` (pare-feu, masquage)
: Si vous avez besoin du masquage, vous devez indiquer `yes` ici. Vos hôtes internes ne sont pas visibles de l'extérieur puisque leurs adresses réseau privées (`192.168.x.x`, par exemple) sont ignorées par les routeurs Internet.

  Pour un pare-feu sans masquage, indiquez `yes` uniquement si vous souhaitez autoriser l'accès au réseau interne. Dans ce cas, vos hôtes internes doivent utiliser des adresses IP officiellement enregistrées. Mais normalement, vous ne devez *pas* autoriser l'accès à votre réseau interne depuis l'extérieur.

FW_MASQUERADE (masquage)
Si vous avez besoin du masquage, vous devez indiquer `yes` ici. Les hôtes internes disposent ainsi d'une connexion quasiment directe à Internet. Pour plus de sécurité, il est préférable d'installer un serveur proxy entre les hôtes du réseau interne et Internet. Le masquage n'est pas nécessaire pour les services fournis par un serveur proxy.

FW_MASQ_NETS (masquage)
Indiquez les hôtes ou les réseaux à masquer, en les séparant par un espace. Par exemple :

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (pare-feu)
Indiquez `yes` si vous souhaitez protéger l'hôte utilisé comme pare-feu contre les tentatives d'attaque en provenance du réseau interne. Pour que les services soient accessibles depuis le réseau interne, vous devez les autoriser explicitement. Consultez également `FW_SERVICES_INT_TCP` et `FW_SERVICES_INT_UDP`.

FW_SERVICES_EXT_TCP (pare-feu)
Indiquez les ports TCP que vous souhaitez rendre disponibles. Laissez ce champ vide s'il s'agit d'un ordinateur personnel qui n'offre aucun service.

FW_SERVICES_EXT_UDP (pare-feu)
Laissez ce champ vide sauf si vous exécutez un service UDP que vous souhaitez rendre accessible de l'extérieur. Parmi les services qui utilisent UDP figurent les serveurs DNS, IPSec, TFTP, DHCP, etc. Dans ce cas, saisissez les ports UDP à utiliser.

FW_SERVICES_INT_TCP (pare-feu)
Cette variable vous permet de définir les services disponibles depuis le réseau interne. La notation est identique à celle employée pour `FW_SERVICES_EXT_TCP`, mais les paramètres s'appliquent au réseau *interne*. Vous ne devez paramétrer cette variable que si `FW_PROTECT_FROM_INT` a pour valeur `yes`.

FW_SERVICES_INT_UDP (pare-feu)
Voir FW_SERVICES_INT_TCP.

Une fois le pare-feu configuré, testez votre configuration. Pour créer les ensembles de règles du pare-feu, entrez `SUSEfirewall2 start` en tant qu'utilisateur `root`. Ensuite, vous pouvez utiliser `telnet`, par exemple, à partir d'un hôte externe, pour

vérifier si la connexion est effectivement refusée. Vous pouvez alors consulter le fichier `/var/log/messages`, qui doit comporter un message semblable à celui-ci :

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

Parmi les autres paquetages disponibles pour tester la configuration de votre pare-feu, citons nmap ou nessus. Vous trouverez la documentation relative à nmap dans `/usr/share/doc/packages/nmap` et la documentation relative à nessus dans le répertoire `/usr/share/doc/packages/nessus-core`, après avoir installé le paquetage correspondant.

23.1.5 Pour plus d'informations

Vous trouverez les informations les plus récentes et la documentation sur le paquetage `SUSEfirewall2` dans `/usr/share/doc/packages/SuSEfirewall2`. La page d'accueil des projets netfilter et iptables (`http://www.netfilter.org`) comporte de nombreux documents, traduits dans plusieurs langues.

23.2 SSH – travailler en réseau en toute sécurité

Lorsque l'on travaille en réseau, il est souvent nécessaire d'accéder à des systèmes depuis des ordinateurs distants. L'utilisateur doit alors s'identifier en envoyant son login et son mot de passe. Si ces données sensibles sont transmises en clair elles risquent d'être interceptées à tout moment par des tiers et d'être utilisées dans l'intérêt de ces derniers en exploitant l'accès de l'utilisateur à son insu. Indépendamment du fait que les attaquants peuvent ainsi prendre connaissance de l'ensemble des données privées de l'utilisateur, ils peuvent utiliser l'accès ainsi obtenu pour attaquer à partir de là d'autres systèmes ou pour usurper les comptes administrateur ou `root` sur le système visé. Dans le passé, c'était le programme telnet, dépourvu de mécanisme de chiffrement ou de sécurité contre l'écoute des liaisons, qui était utilisé pour connecter deux machines distantes. De même, d'autres canaux de communication, comme les connexions FTP simples et certaines copies entre machines distantes, ne sont pas protégées.

Le programme SSH apporte la protection requise en chiffrant les données d'authentification (généralement un nom d'utilisateur et un mot de passe) ainsi que les autres données échangée. Même s'il reste possible, pour un tiers, d'intercepter les données transmises, leur contenu ne peut pas être déchiffré, faute de disposer de la clé appropriée. Cette méthode permet ainsi des communications sécurisées sur des réseaux non sécurisés tels que le réseau Internet. SUSE Linux propose pour cela le paquetage OpenSSH.

23.2.1 Le paquetage OpenSSH

Le paquetage OpenSSH est installé par défaut sous SUSE Linux. Vous disposez ainsi des programmes ssh, scp et sftp, afin de remplacer telnet, rlogin, rsh, rcp et ftp. Dans la configuration par défaut, l'accès à un système SUSE Linux n'est possible qu'avec les utilitaires OpenSSH et uniquement si le pare-feu autorise l'accès.

23.2.2 Le programme ssh

Le programme ssh permet de se connecter à un système distant et d'y travailler de façon interactive. Il constitue ainsi une alternative à telnet et à rlogin. Le programme slogin n'est qu'un lien symbolique faisant référence à ssh. Ainsi, la commande `ssh sun` permet de se connecter sur la machine sun. L'hôte invite alors à entrer le mot de passe pour le système sun.

Une fois authentifié, vous pouvez alors y travailler soit à partir de la ligne de commande soit en mode graphique, par exemple avec YaST. Dans le cas où votre nom d'utilisateur sur la machine locale et celui sur le système distant sont différents, vous pouvez spécifier un autre nom, par exemple `ssh -l augustine sun` ou `ssh augustine@sun`.

D'autre part, le programme ssh offre une possibilité connue avec rsh et consistant à exécuter des commandes sur un autre système. Dans l'exemple suivant, la commande `uptime` est exécutée sur la machine sun et un répertoire nommé `tmp` est créé. Le programme affiche sur le terminal local de la machine earth.

```
ssh soleil "uptime; mkdir tmp"
tux@soleil's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Dans cette commande, les guillemets sont requis afin de regrouper les deux instructions en une commande unique. C'est nécessaire pour permettre l'exécution de la seconde commande sur la machine sun.

23.2.3 scp—Copie sécurisée

Le programme scp vous permet de copier des fichiers sur une machine distante. scp constitue une alternative sécurisée et chiffrée au programme rcp. Ainsi, la commande `scp MonCourrier.tex sun:` copie le fichier `MonCourrier.tex` de la machine earth sur la machine sun. Dans le cas où le nom d'utilisateur sur earth est différent de celui sur sun, utilisez pour la commande scp la notation `NomUtilisateur@NomMachine`. L'option `-l` n'est pas disponible.

Après avoir saisi votre mot de passe, le programme scp commence à transférer les données en affichant l'avancement à l'aide d'une jauge formée d'astérisques et progressant de gauche à droite. Dans le même temps, la durée estimée restant jusqu'à la fin de la transmission (estimated time of arrival) est affichée sur la droite. Il est également possible d'inhiber l'affichage à l'aide de l'option `-q`.

La copie de fichiers individuels n'est pas la seule opération que scp permet d'effectuer. En effet, il est également possible de transférer récursivement des répertoires entiers : ainsi, la commande `scp -r src/ sun:backup/` copie la totalité du répertoire `src/`, y compris les sous-répertoires présents sur la machine sun, dans le sous-répertoire `backup/`. Ce dernier est créé automatiquement s'il n'existe pas encore.

L'option `-p` permet à scp de conserver l'horodatage des fichiers. L'option `-C` permet de compresser les fichiers à transférer, ce qui, d'un côté, permet de réduire le volume de données à transférer, mais de l'autre, impose une charge supérieure au système.

23.2.4 sftp—Transfert de fichiers sécurisé

On peut aussi utiliser le programme sftp pour transférer les données de façon sécurisée. sftp propose une session à l'intérieur de laquelle on peut utiliser plusieurs des commandes ftp bien connues. Par rapport à scp, le principal avantage est de pouvoir transférer des données lorsqu'on ne connaît pas le nom de fichier.

23.2.5 Le démon SSH (sshd)—côté serveur

Pour pouvoir fonctionner, ssh et scp, les programmes clients du paquetage SSH ont besoin que le démon SSH qui est un serveur s'exécute en arrière-plan. Celui-ci attend les connexions sur le `port TCP/IP numéro 22`. La première fois qu'il est

démarré, le démon génère trois paires de clés. Celles-ci comportent une partie privée et une partie publique (public). il s'agit donc d'une méthode à clé publique. Pour assurer la sécurité de l'application à l'aide de SSH, seul l'administrateur doit pouvoir voir les fichiers de la clé privée. Les privilèges correspondant sont définis par défaut de manière restrictive. Les clés privées sont utilisées en local uniquement par le démon SSH et ne doivent être communiquées à personne. En revanche, la partie publique de la clé (identifiable par l'extension de fichier `.pub`) peut être communiquée à vos correspondants et peut être lue par tous les utilisateurs.

Une connexion est créée par le client SSH. Le démon SSH en attente et le client SSH à l'origine de la demande échangent des données d'identification en vue de comparer la version du protocole et du logiciel et d'éviter une connexion sur un mauvais port. La réponse étant apportée par un processus fils du démon SSH initial, il est possible d'avoir plusieurs connexions SSH simultanément.

Afin d'assurer la communication entre le serveur SSH et le client SSH, le programme OpenSSH prend en charge les versions 1 et 2 du protocole SSH. Après avoir réinstallé SUSE Linux, c'est la version 2 actuelle du protocole qui est automatiquement utilisée. Si vous souhaitez continuer à utiliser SSH1 après une mise à jour, veuillez suivre les instructions données dans `/usr/share/doc/packages/openssh/README.SuSE`. Vous y trouverez également la marche à suivre pour passer d'un environnement SSH 1 à un environnement SSH 2 opérationnel.

Si vous utilisez le protocole SSH version 1, le serveur envoie sa clé d'hôte (en anglais, host key) publique ainsi qu'une clé de serveur (en anglais, server key) générée toutes les heures par le démon SSH. Grâce à ces deux clés, le client SSH chiffre une clé de session (en anglais, session key) et l'envoie au serveur SSH.Il communique par ailleurs au serveur la méthode de chiffrement choisie.

Le protocole SSH version 2 fonctionne sans la clé de serveur. Ce dispositif est remplacé par un algorithme de Diffie-Hellman destiné à l'échange des clés.

Il n'est pas possible de déduire les clés privées de l'hôte et du serveur, indispensables pour déchiffrer la clé de session, à partir des parties publiques de la clé. Ainsi, seul le démon SSH contacté est en mesure de déchiffrer la clé de session à l'aide de ses clés privées (voir `man /usr/share/doc/packages/openssh/RFC.nroff`). Cette phase préparatoire de la connexion peut être aisément tracée à l'aide de l'option de débogage `-v` du programme client SSH.

Par défaut, c'est la version 2 du protocole SSH qui est utilisée, même si le paramètre `-1` permet d'imposer la version 1 du protocole SSH. En stockant après le premier contact toutes les clés publiques dans `~/.ssh/known_hosts`, il est possible de contrer les attaques de type interception (man-in-the-middle). Les serveurs SSH tentant d'usurper le nom et l'adresse IP d'un autre sont démasqués avec un avertissement sans ambiguïté. Ils sont identifiés par leur clé d'hôte différente de `~/.ssh/known_hosts` ou sont dans l'impossibilité de déchiffrer la clé de session convenue, faute de connaître la partie privée adéquate.

Il est recommandé d'archiver sur un support externe et en les protégeant comme il se doit les clés privées et publiques de `/etc/ssh/`. Vous pouvez ainsi constater d'éventuelles modifications apportées aux clés et récupérer les anciennes clés dans le cas où vous auriez à réinstaller votre système. Cette précaution épargnera aux utilisateurs l'inquiétude que peuvent causer des messages d'avertissement. Dans le cas où vous avez la certitude d'avoir à faire au bon serveur SSH en dépit de l'avertissement, la ligne existante correspondant au système doit être retirée du fichier `~/.ssh/known_hosts`.

23.2.6 Mécanismes d'authentification de SSH

L'authentification proprement dite intervient à cet instant. Sous sa forme la plus simple, elle consiste à saisir un mot de passe, de manière analogue à la procédure illustrée dans les exemples précédents. L'objet de SSH était de mettre en place un logiciel sécurisé tout en restant simple à utiliser. Comme il visait à remplacer les programmes rsh et rlogin, SSH devait offrir une méthode d'authentification simple à utiliser au quotidien. Cet objectif est réalisé par SSH à l'aide d'une autre paire de clés générée ici par l'utilisateur. Le paquetage SSH offre pour cela l'utilitaire ssh-keygen. La paire de clés est générée après avoir saisi `ssh-keygen -t rsa` ou `ssh-keygen -t dsa` et vous devez indiquer un nom pour le fichier de base destiné à stocker les clés.

Validez la valeur par défaut et lorsque l'on vous demande une phrase de passe, donnez-en une. Même si le logiciel accepte une phrase de passe vide, nous conseillons de choisir un texte de 10 à 30 signes. Dans la mesure du possible, évitez d'utiliser des mots ou phrases courts et simples. Après la saisie, vous devez vérifier la première saisie en effectuant une seconde saisie. Vous devez ensuite indiquer l'emplacement de la clé privée et publique, en l'occurrence les fichiers `id_rsa` et `id_rsa.pub`.

Utilisez la commande `ssh-keygen -p -t rsa` ou `ssh-keygen -p -t dsa` pour modifier votre ancienne phrase de passe. Copiez la partie publique de la clé (dans notre exemple `id_rsa.pub`) sur la machine distante et enregistrez-la sous `~/.ssh/authorized_keys`. Lors de la prochaine connexion, vous devrez saisir votre phrase de passe. Dans le cas contraire, vérifiez l'emplacement et le contenu des fichiers dont il vient d'être question.

À la longue, cette procédure s'avère plus lourde que celle consistant à saisir un mot de passe. Le paquetage SSH s'accompagne d'un utilitaire supplémentaire, ssh-agent, proposant des clés privées valables pour la durée d'une session X. Pour cela, le programme X est démarré comme processus fils de ssh-agent. La méthode la plus simple pour mettre cette fonctionnalité en place consiste à placer au début du fichier `.xsession` la variable `usessh` en fixant sa valeur à `yes` et à vous connecter à partir d'un gestionnaire de connexions tel que KDM ou XDM. Une autre possibilité est d'entrer `ssh-agent startx`.

Vous pouvez à présent utiliser ssh ou scp comme à l'accoutumée. Si vous avez partagé votre clé publique comme indiqué précédemment, vous devriez être dispensé de donner votre mot de passe. Lorsque vous vous éloignez de votre ordinateur, prenez toutefois la précaution de terminer votre session X ou de la verrouiller à l'aide d'un économiseur d'écran protégé par mot de passe, par exemple xlock.

Toutes les modifications importantes résultant de l'utilisation du protocole SSH version 2 sont également récapitulées dans le fichier `/usr/share/doc/packages/openssh/README.SuSE`.

23.2.7 Mécanismes de redirections, d'authentification et X

Indépendamment des améliorations en matière de sécurité dont il vient d'être question, le programme ssh facilite également l'utilisation d'applications X distantes. Lorsque vous appelez `ssh` avec l'option `-X`, la variable DISPLAY est automatiquement définie sur le système distant et toutes les sorties X sont redirigées vers la machine source à travers la connexion ssh existante. Cette fonctionnalité pratique interdit dans le même temps les possibilités d'écoute qui existaient auparavant, lorsque l'on appelait à distance des applications X pour les afficher en local.

En définissant l'option -A, le mécanisme d'authentification de l'agent ssh-agent est repris sur la machine suivante. Vous pouvez ainsi passer d'une machine à l'autre sans être obligé de saisir de mot de passe. Ceci n'est toutefois possible que si vous avez préalablement copié et convenablement enregistré votre clé publique sur les machines cibles concernées.

Par précaution, les deux mécanismes sont désactivés par défaut, même s'ils peuvent être activés de manière permanente dans le fichier de configuration système /etc/ssh/ssh_config ou dans le fichier utilisateur ~/.ssh/config.

Le programme ssh peut également être utilisé afin de permettre des redirections de connexions TCP/IP. Exemple d'application : la redirection des ports SMTP et POP3 :

```
ssh -L 25:sun:25 earth
```

Dans cet exemple, toutes les connexions vers *earth port 25* (SMTP) sont redirigées vers le port SMTP de sun via un canal chiffré. Cette possibilité est particulièrement utile pour les utilisateurs de serveurs SMTP dépourvus de fonctions SMTP-AUTH ou POP-before-SMTP. Ainsi, le courrier peut être transmis de n'importe quel endroit disposant d'une connexion réseau afin d'être acheminé par le serveur de messagerie domestique. De manière analogue, la commande suivante permet de rediriger toutes les requêtes POP3 (port 110) adressées à earth vers le port POP3 de sun :

```
ssh -L 110:sun:110 earth
```

Vous devez exécuter ces deux exemples en tant qu'utilisateur root, la connexion s'effectuant sur des ports locaux privilégiés. Lorsque la connexion SSH est établie, l'utilisateur envoie et reçoit les messages à partir de son compte habituel. L'hôte SMTP et POP3 doit être configuré à localhost. Vous trouverez des informations complémentaires dans les pages de manuels des différents programmes et dans les fichiers sous /usr/share/doc/packages/openssh.

23.3 Codage des partitions et des fichiers

Tout utilisateur dispose de certaines données confidentielles dont l'accès doit être interdit aux tiers. Plus vous travaillez en réseau ou plus vous vous déplacez, plus vous devez traiter ces données avec précaution. Le codage de fichiers ou de partitions entières est

recommandé si d'autres personnes y ont accès par une connexion réseau ou un accès physique direct.

AVERTISSEMENT: Les supports codés offrent une protection limitée

Attention : les méthodes décrites dans cette section ne vous permettent pas de protéger votre système contre les tentatives d'attaque lorsqu'il est actif. Après le montage réussi des supports codés, tout utilisateur doté des autorisations adéquates peut y accéder. Le codage de support prend tout son sens si vous perdez votre ordinateur ou s'il est volé et que des utilisateurs non autorisés souhaitent lire vos données confidentielles.

Voici un certain nombre de scénarios d'utilisation possibles.

Ordinateurs portables
: Si vous vous déplacez avec votre ordinateur portable, il peut s'avérer judicieux de coder les partitions du disque dur contenant des données confidentielles. Si vous perdez votre ordinateur portable ou s'il est volé, vos données seront protégées si elles sont stockées dans un système de fichiers codé ou dans un fichier codé unique.

Supports amovibles
: Les lecteurs flash USB ou les disques durs externes sont tout aussi susceptibles d'être volés que les ordinateurs portables. Un système de fichiers codé fournit une protection contre un accès tiers.

Postes de travail
: Dans les entreprises où presque tout le monde a accès à votre ordinateur, il peut s'avérer utile de coder une partition ou des fichiers individuels.

23.3.1 Configuration d'un système de fichiers codé avec YaST

YaST permet de coder des fichiers ou des partitions au cours de l'installation, ainsi que sur un système déjà installé. Un fichier codé peut être créé à tout moment car il s'adapte parfaitement à tout schéma de partitionnement existant. Pour coder intégralement une partition, dédiez la partition en question dans le schéma de partitionnement. La proposition de partitionnement standard de YaST ne comprend pas de partition codée par défaut. Ajoutez-la manuellement dans la boîte de dialogue de partitionnement.

Création d'une partition codée au cours de l'installation

AVERTISSEMENT: Saisie du mot de passe

Prenez en compte les avertissements sur la sécurité par mot de passe lorsque vous définissez le mot de passe des partitions codées et mémorisez-le correctement. Sans le mot de passe, vous ne pouvez ni accéder aux données codées, ni les restaurer.

Décrite à la Section « Partitionnement » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage), la boîte de dialogue YaST de partitionnement pour experts propose les options nécessaires à la création d'une partition codée. Cliquez sur *Créer* comme pour créer une partition normale. Dans la boîte de dialogue qui apparaît, entrez les paramètres de la nouvelle partition, notamment le formatage et le point de montage souhaités. Achevez le processus en cliquant sur *Système de fichiers crypté*. Dans la boîte de dialogue suivante, entrez deux fois le mot de passe. La nouvelle partition codée est créée dès que vous cliquez sur *OK* pour fermer la boîte de dialogue de partitionnement. Lors du démarrage, le système d'exploitation demande le mot de passe avant de monter la partition.

Si vous ne souhaitez pas monter la partition codée au démarrage, appuyez sur Entrée lorsque vous êtes invité à saisir le mot de passe. Refusez ensuite d'entrer à nouveau le mot de passe. Dans ce cas, le système de fichiers codé n'est pas monté et le système d'exploitation poursuit le démarrage en bloquant l'accès à vos données. La partition est disponible à tous les utilisateurs dès qu'elle a été montée.

Si le système de fichiers codé ne doit être monté qu'au cas par cas, activez *Ne pas monter au démarrage du système* dans la boîte de dialogue *Options Fstab*. La partition correspondante ne sera pas montée lors du démarrage du système. Pour la rendre disponible ultérieurement, montez-la manuellement avec `mount` *`nom de la partition point de montage`*. Entrez le mot de passe lorsque vous y êtes invité. Après avoir terminé votre travail sur la partition, démontez-la avec `umount nom de la partition` pour empêcher les autres utilisateurs d'y accéder.

Création d'une partition codée sur un système en cours d'exécution

---

AVERTISSEMENT: Activation du codage sur un système en cours d'exécution

Il est également possible de créer des partitions codées sur un système en cours d'exécution, notamment au cours de l'installation. Cependant, le codage d'une partition existante détruit toutes les données qu'elle contient.

Sur un système en cours d'exécution, sélectionnez *Système → Partitionnement* dans le centre de contrôle YaST. Cliquez sur *Oui* pour poursuivre. Au lieu de sélectionner *Créer* comme dans la procédure ci-dessus, cliquez sur *Modifier*. Le reste de la procédure est identique.

Installation de fichiers codés

Au lieu d'utiliser une partition codée, vous avez la possibilité de créer des systèmes de fichiers codés au sein de fichiers individuels pour conserver des données confidentielles. Ces derniers sont créés à partir de la même boîte de dialogue YaST. Sélectionnez *Fichier chiffrement* et entrez le chemin du fichier à créer ainsi que la taille souhaitée. Acceptez les paramètres de formatage proposés et le type de système de fichiers. Indiquez ensuite le point de montage et si le système de fichiers codé doit être monté au démarrage du système.

L'avantage des fichiers codés est qu'ils peuvent être ajoutés sans repartitionner le disque dur. Ils sont montés à l'aide d'un périphérique de bouclage (loop) et se comportent comme des partitions normales.

Utilisation de vi pour coder des fichiers

L'utilisation de partitions codées présente un inconvénient. En effet, tant que la partition est montée, l'utilisateur `root` peut toujours accéder aux données. Pour contourner ce problème, vous pouvez utiliser vi en mode codé.

Utilisez `vi -x` *`nom de fichier`* pour modifier un nouveau fichier. vi vous demande de définir un mot de passe et code ensuite le contenu du fichier. Chaque fois que vous accédez à ce fichier, vi demande le mot de passe correct.

Pour une sécurité accrue, vous pouvez placer le fichier texte codé dans une partition codée. Cette opération est recommandée car le codage utilisé dans vi n'est pas très pointu.

23.3.2 Codage du contenu d'un support amovible

YaST considère les supports amovibles comme des disques durs externes ou les lecteurs flash USB comme tout autre disque dur. Les fichiers ou les partitions sur ce type de support peuvent être codés selon la procédure ci-dessus. Toutefois, ne montez pas ces supports lors du démarrage du système car ils ne sont, en principe, connectés que lorsque le système est en cours d'exécution.

23.4 Sécurité et confidentialité

L'une des principales caractéristiques d'un système Linux ou UNIX est sa capacité à gérer plusieurs utilisateurs simultanément et à les autoriser à effectuer plusieurs tâches en même temps sur le même ordinateur. De plus, le système d'exploitation est transparent vis-à-vis du réseau. Ainsi, il arrive fréquemment que les utilisateurs ne sachent pas si les données et les applications qu'ils utilisent sont fournies localement à partir de leur machine ou si elles sont mises à disposition via le réseau.

Si vous utilisez la fonctionnalité multi-utilisateur, les données des différents utilisateurs doivent être stockées séparément. La sécurité et la confidentialité doivent être garanties. La sécurité des données a toujours été un sujet important, même avant que les ordinateurs soient reliés en réseau. Tout comme aujourd'hui, la principale préoccupation était de pouvoir conserver les données malgré la perte ou la défaillance du support de données, généralement le disque dur.

Cette section concerne essentiellement la confidentialité des données et la protection de la vie privée de l'utilisateur. Rappelons tout de même qu'une politique de sécurité globale doit toujours comprendre un système de sauvegarde régulier, éprouvé et en bon état de marche. Sans cela, vous risquez d'avoir de grandes difficultés à récupérer vos données en cas de défaillance matérielle ou si vous suspectez un individu d'avoir accédé de façon frauduleuse à vos fichiers, et de les avoir manipulés ou modifiés.

23.4.1 Sécurité locale et sécurité réseau

Il existe plusieurs moyens d'accéder aux données :

- la communication personnelle avec les individus qui possèdent les informations souhaitées ou accèdent aux données sur un ordinateur ;
- directement à partir de la console d'un ordinateur (accès physique) ;
- via une ligne série ;
- à l'aide d'une connexion réseau.

Quelle que soit la situation, l'utilisateur doit être authentifié pour pouvoir accéder aux ressources ou aux données en question. À cet égard, un serveur Web peut être moins limité mais vous ne souhaitez pas pour autant qu'il divulgue toutes vos données personnelles à n'importe quel internaute.

Le premier des cas mentionnés ci-dessus est celui qui fait le plus appel au facteur humain, comme lorsque vous êtes en relation avec un employé de banque et que vous devez prouver que vous êtes le titulaire du compte bancaire. Il vous demande alors de fournir une signature, un numéro d'identification ou un mot de passe pour prouver que vous êtes la personne que vous affirmez être. Il est parfois possible de soutirer des renseignements à une personne informée, en mentionnant simplement quelques fragments d'informations connues pour gagner sa confiance grâce à une rhétorique intelligente. La victime peut être amenée à révéler progressivement davantage d'informations, peut-être même sans en avoir conscience. Les pirates informatiques appellent cette technique l'*ingénierie sociale* (social engineering en anglais). Contre ce type d'attaque, le seul remède consiste à éduquer les personnes, à manipuler avec précaution vos informations et à prendre garde aux renseignements que vous communiquez. Avant de pénétrer dans les systèmes informatiques, les pirates tentent souvent de s'attaquer aux réceptionnistes, aux prestataires de services de la société, voire aux membres de la famille. Basées sur l'ingénierie sociale, ces attaques ne sont généralement découvertes que bien plus tard.

Une personne qui souhaite accéder à vos données de manière illégale peut également utiliser la méthode traditionnelle et tenter de pénétrer directement dans votre ordinateur. Vous devez donc le protéger contre toute falsification, afin que personne ne puisse supprimer, remplacer ou bloquer ses composants. Cette règle s'applique également aux sauvegardes, et même aux câbles réseau ou aux câbles d'alimentation. Vous devez également sécuriser la procédure d'amorçage puisque des combinaisons de touches

connues peuvent provoquer un comportement anormal. Pour vous protéger, créez des mots de passe pour le BIOS et le chargeur d'amorçage.

Les terminaux série reliés aux ports série sont encore fréquemment utilisés aujourd'hui. Contrairement aux interfaces réseau, ils n'ont pas recours à un protocole réseau pour communiquer avec l'hôte. Un simple câble ou un port infrarouge permet de transmettre du texte en clair entre les périphériques. Le câble est le maillon faible de ce type de système : il suffit d'y connecter une vieille imprimante pour enregistrer tout ce qui passe par les câbles. Ce que l'on peut faire avec une imprimante peut aussi être effectué différemment, selon les efforts mis en œuvre dans le cadre de l'attaque.

La lecture locale d'un fichier sur un hôte requiert l'application d'autres règles d'accès que l'ouverture d'une connexion réseau avec un serveur sur un hôte différent. Il y a une différence entre sécurité locale et sécurité réseau. Cette différence est le point où les données doivent être mises en paquets pour pouvoir être envoyées ailleurs.

Sécurité locale

La sécurité locale commence par l'environnement physique du lieu où est situé l'ordinateur. Installez votre machine à un endroit où la sécurité est conforme à vos attentes et vos besoins. La sécurité locale vise essentiellement à séparer les utilisateurs les uns des autres, de façon à ce qu'aucun d'eux ne puisse deviner les autorisations ou l'identité d'un autre. Il s'agit d'une règle générale à respecter mais qui s'applique plus particulièrement à l'utilisateur `root`, qui possède les pleins pouvoirs sur le système. Il peut ainsi prendre l'identité de n'importe quel autre utilisateur local sans devoir saisir de mot de passe et lire tous les fichiers locaux.

Mots de passe

Sous Linux, les mots de passe ne sont pas stockés en clair et la chaîne de caractères saisie n'est pas simplement mise en correspondance avec le modèle enregistré. Si tel était le cas, tous les comptes de votre système seraient exposés à un risque dès qu'un individu accéderait au fichier correspondant. C'est pourquoi chaque mot de passe stocké est codé. Il est de nouveau codé lors de chaque saisie et les deux chaînes codées sont comparées. Cette technique n'est utile que s'il est impossible de recomposer le mot de passe en clair à partir du mot de passe codé.

On utilise à cet effet un algorithme particulier, appelé *algorithme à trappe*, parce qu'il ne fonctionne que dans un sens. Un pirate qui s'est emparé de la chaîne codée ne peut

pas obtenir votre mot de passe en appliquant simplement le même algorithme. Il lui faudrait tester toutes les combinaisons de caractères possibles jusqu'à ce qu'il trouve une combinaison similaire à votre mot de passe lorsqu'il est codé. Avec des mots de passe de huit caractères, il existe un nombre considérable de combinaisons possibles.

Dans les années 70, cette méthode était considérée comme la plus sûre en raison de la vitesse relative de l'algorithme utilisé, qui mettait quelques secondes à coder un mot de passe. Depuis, les ordinateurs sont devenus suffisamment puissants pour effectuer plusieurs centaines de milliers, voire plusieurs millions de codages par seconde. C'est pourquoi les utilisateurs standard ne doivent pas avoir accès aux mots de passe codés (ils ne peuvent pas lire le fichier `/etc/shadow`). Il est encore plus important que les mots de passe ne soient pas faciles à deviner, au cas où le fichier de mots de passe deviendrait accidentellement visible. Il n'est donc pas vraiment utile de « transformer » un mot de passe comme « intrigue » en « 1ntr1gu3 ».

Le remplacement de certaines lettres d'un mot par des chiffres qui leur ressemblent n'est pas suffisant. Les programmes de craquage qui utilisent des dictionnaires pour deviner les mots de passe connaissent ce genre de remplacement. Il est donc plus judicieux de créer un mot qui n'a aucun sens, sauf pour vous, par exemple les premières lettres d'une phrase ou le titre d'un livre, comme « Le Nom de la Rose » d'Umberto Eco. Vous obtiendriez un mot de passe très sûr : « LNdlRdUE ». En revanche, des mots de passe tels que « bordeaux » ou « xavier76 » pourraient facilement être devinés par quelqu'un qui vous connaît, ne serait-ce que superficiellement.

La procédure d'amorçage

Configurez votre système de façon à interdire tout démarrage à partir d'une disquette ou d'un CD. Pour ce faire, supprimez les lecteurs correspondants ou définissez un mot de passe BIOS et configurez le BIOS pour n'autoriser l'amorçage qu'à partir du disque dur. Un système Linux est généralement démarré par un chargeur d'amorçage, ce qui vous permet de transmettre des options supplémentaires au kernel démarré. Pour éviter que des tiers utilisent ces paramètres lors de l'amorçage, créez un mot de passe supplémentaire dans `/boot/grub/menu.lst` (consultez le Chapitre 29, *Chargeur d'amorçage* (p. 471)). Cette procédure est déterminante pour la sécurité de votre système. Le kernel lui-même est exécuté avec les autorisations `racine (root)` mais c'est également la première autorité qui accorde des autorisations de ce type lors du démarrage du système.

Autorisations de fichier

En règle générale, utilisez toujours les privilèges les plus restrictifs pour une tâche donnée. Par exemple, il n'est absolument pas nécessaire d'être un utilisateur `root` pour lire ou écrire un message. Si le programme de messagerie comporte un bogue, celui-ci peut être exploité pour une attaque qui agit alors avec exactement les mêmes autorisations que celles que vous aviez au lancement du programme. Vous limiterez les éventuels dégâts en suivant la règle ci-dessus.

Les autorisations associées aux plus de 200 000 fichiers inclus dans la distribution SUSE font l'objet d'un choix minutieux. Un administrateur système qui installe des logiciels supplémentaires ou d'autres fichiers doit être particulièrement prudent, notamment lorsqu'il définit les bits d'autorisation. Les administrateurs expérimentés et soucieux de la sécurité utilisent toujours l'option `-l` avec la commande `ls` pour obtenir une longue liste de fichiers, ce qui leur permet de détecter immédiatement toute autorisation de fichier incorrecte. Un attribut de fichier incorrect ne signifie pas uniquement que les fichiers ont pu être modifiés ou supprimés. Ces fichiers modifiés peuvent être exécutés par l'utilisateur `root` ou, dans le cas des fichiers de configuration, des programmes peuvent les utiliser avec les autorisations de l'utilisateur `root`. Cela offre encore plus de possibilités aux pirates informatiques. On appelle ce genre d'attaque des oeufs de coucou parce que le programme (l'oeuf) est exécuté (couvé) par un utilisateur étranger (l'oiseau), un peu comme un coucou se débrouille pour faire couver ses oeufs par d'autres oiseaux.

Un système SUSE Linux contient les fichiers `permissions`, `permissions.easy`, `permissions.secure` et `permissions.paranoid`, tous situés dans le répertoire `/etc`. Le but de ces fichiers est de définir des autorisations spéciales, notamment des répertoires pour lesquels tout utilisateur dispose de droits en écriture ou, pour les fichiers, le bit « setuser ID ». Grâce à ces bits de changement d'identité, un programme ne s'exécute pas avec les autorisations de l'utilisateur qui l'a démarré mais avec celles du propriétaire du fichier, qui est généralement l'utilisateur `root`. Un administrateur peut utiliser le fichier `/etc/permissions.local` pour ajouter ses propres paramètres.

Pour déterminer, parmi les fichiers ci-dessus, ceux qui seront utilisés par les programmes de configuration de SUSE pour définir les autorisations, sélectionnez *Sécurité* dans YaST. Pour en savoir plus à ce sujet, lisez les commentaires de `/etc/permissions` ou consultez la page du manuel sur `chmod` (`man chmod`).

Dépassement de tampon et bogues de chaîne de format

Vous devez être particulièrement attentif lorsqu'un programme est censé traiter des données susceptibles d'être modifiées par un utilisateur. Toutefois, ce conseil s'adresse davantage aux programmeurs d'application qu'aux utilisateurs standard. Le programmeur doit s'assurer que son application interprète correctement les données, sans les écrire dans un espace mémoire trop petit. En outre, le programme doit transmettre les données de façon homogène, à l'aide des interfaces définies à cet effet.

Un *dépassement de tampon* peut se produire si la taille réelle de la mémoire tampon n'est pas prise en compte lors de l'écriture des données dans ce tampon. Dans certains cas, ces données (telles qu'elles sont générées par l'utilisateur) utilisent plus d'espace que l'espace disponible dans le tampon. Les données sont donc écrites au-delà de l'extrémité de cette zone de tampon. Ainsi, il arrive qu'un programme soit en mesure d'exécuter des séquences de programme choisies par l'utilisateur (et non par le programmeur), au lieu de traiter simplement les données de l'utilisateur. Ce type de bogue peut avoir de graves conséquences, notamment si le programme est exécuté avec des privilèges particuliers (consultez la section intitulée « Autorisations de fichier » (p. 366)).

Le fonctionnement des *bogues de chaîne de format* est légèrement différent mais, là encore, les données saisies par l'utilisateur peuvent détourner le programme. Ces erreurs de programmation sont généralement exploitées par les programmes exécutés avec des autorisations spéciales, comme par exemple les programmes setuid et setgid. Vous pouvez donc protéger votre système et vos données contre ce type de bogue, en supprimant les autorisations d'exécution correspondantes des programmes. La meilleure méthode est encore une fois d'appliquer la règle d'utilisation des privilèges les plus limités possibles (consultez la section intitulée « Autorisations de fichier » (p. 366)).

Le dépassement de tampon et les bogues de chaîne de format sont des bogues liés à la gestion des données utilisateur. Ils ne sont donc pas uniquement exploitables si l'accès a été accordé à un compte local. En effet, la plupart des bogues connus peuvent aussi être exploités sur une liaison réseau. Par conséquent, le dépassement de tampon et les bogues de chaîne de format concernent aussi bien la sécurité locale que la sécurité réseau.

Virus

Contrairement à ce que l'on pense, certains virus peuvent être exécutés sous Linux. Toutefois, les virus connus ont été créés par leurs auteurs dans le cadre d'une *validation technique*, pour démontrer que la technique fonctionne comme prévu. Jusqu'à présent, aucun de ces virus n'a été détecté *dans la nature*.

Pour se propager, les virus ont besoin d'un hôte, sans lequel ils ne peuvent pas survivre. Cet hôte est un programme ou une importante zone de stockage du système, comme le secteur d'amorçage principal, sur lequel le code programme du virus doit pouvoir écrire. Du fait de ses fonctionnalités multi-utilisateurs, Linux peut limiter l'accès en écriture à certains fichiers, et notamment aux fichiers système. Par conséquent, si vous travaillez en tant qu'utilisateur `root`, vous augmentez le risque d'infecter votre système avec ce type de virus. En revanche, si vous respectez le principe qui consiste à utiliser les privilèges les plus limités possibles, comme indiqué ci-dessus, le risque d'infection est faible.

D'autre part, vous devez toujours être prudent avant d'exécuter un programme provenant d'un site Internet que vous ne connaissez pas vraiment. Les paquetages RPM de SUSE comportent une signature cryptographique qui démontre le soin avec lequel ils ont été élaborés. Les virus prouvent généralement que l'administrateur ou l'utilisateur n'accorde pas une attention suffisante à la sécurité, et met en péril un système dont la conception même devrait lui conférer une sécurité à toute épreuve.

Ne confondez pas les virus et les vers, qui appartiennent entièrement au monde des réseaux. Les vers n'ont pas besoin d'un hôte pour se propager.

Sécurité réseau

La sécurité réseau permet de se protéger contre les attaques provenant de l'extérieur. La procédure de login classique, qui exige l'authentification de l'utilisateur à l'aide d'un nom d'utilisateur et d'un mot de passe, reste un problème de sécurité locale. En cas de login via un réseau, vous devez différencier les deux aspects de la sécurité. Ce qui se passe jusqu'à l'authentification proprement dite correspond à la sécurité réseau et tout ce qui se passe après correspond à la sécurité locale.

Système X Window et authentification X

Comme nous l'avons vu, la transparence du réseau est une caractéristique fondamentale du système UNIX. Elle l'est d'autant plus avec X, le système de fenêtrage des systèmes d'exploitation UNIX. En effet, vous n'aurez aucun problème pour vous loguer à un hôte distant et lancer un programme graphique, qui sera ensuite envoyé sur le réseau pour s'afficher sur votre ordinateur.

Si vous souhaitez afficher un client X à distance à l'aide d'un serveur X, ce dernier doit protéger les ressources qu'il gère (l'affichage) contre les accès non autorisés. En d'autres termes, certaines autorisations doivent être octroyées au programme client. X Window propose deux méthodes : le contrôle d'accès basé sur l'hôte et le contrôle d'accès basé sur les cookies. La première a recours à l'adresse IP de l'hôte sur lequel le client doit être exécuté. Cette opération est assurée par le programme xhost, qui entre l'adresse IP d'un client légitime dans une minuscule base de données qui appartient au serveur X. L'authentification à l'aide d'adresses IP n'est toutefois pas très sûre. Par exemple, en cas de présence d'un deuxième utilisateur travaillant sur l'hôte qui envoie le programme client, il aurait également accès au serveur X, comme une personne qui déroberait l'adresse IP. En raison de ces défauts, nous ne décrirons pas cette méthode d'authentification plus en détail. Pour en savoir plus, consultez la page du manuel sur `man xhost`.

Dans le cadre du contrôle d'accès basé sur les cookies, une chaîne de caractères connue uniquement par le serveur X et l'utilisateur autorisé est générée, un peu comme un badge d'identification. Le mot anglais cookie signifie biscuit et désigne ici les biscuits porte-bonheur chinois qui contiennent une maxime. Ce cookie est enregistré lors du login dans le fichier `.Xauthority` (dans le répertoire privé de l'utilisateur) et est mis à disposition de tout client X qui souhaite utiliser le serveur X pour afficher une fenêtre. L'utilisateur peut examiner le fichier `.Xauthority` à l'aide de l'outil xauth. Si vous renommez `.Xauthority` ou si vous le supprimez accidentellement de votre répertoire privé, vous ne pouvez plus ouvrir aucune nouvelle fenêtre ni aucun client X. Pour plus d'informations sur les mécanismes de sécurité du système X Window, consultez la page du manuel sur Xsecurity (`man Xsecurity`).

SSH (shell sécurisé) permet de coder complètement une connexion réseau et de la rediriger vers un serveur X de façon transparente, sans que le mécanisme de codage soit perçu par l'utilisateur. Cette opération est également appelée redirection X. La redirection X est réalisée en simulant un serveur X du côté serveur et en définissant une variable DISPLAY pour le shell sur l'hôte distant. Pour plus d'informations sur SSH, consultez la Section 23.2, « SSH – travailler en réseau en toute sécurité » (p. 352).

AVERTISSEMENT

Si vous pensez que l'hôte auquel vous vous loguez n'est pas sûr, n'utilisez pas la redirection X. Lorsque la redirection X est activée, un pirate peut s'authentifier via votre connexion SSH pour pénétrer dans votre serveur X et épier votre clavier, par exemple.

Dépassement de tampon et bogues de chaîne de format

Comme l'indique la section intitulée « Dépassement de tampon et bogues de chaîne de format » (p. 367), le dépassement de tampon et les bogues de chaîne de format concernent aussi bien la sécurité locale que la sécurité réseau. Comme pour les variantes locales de ces types de bogues, le dépassement de tampon des programmes réseau est essentiellement utilisé pour s'octroyer les autorisations `racine (root)`, s'il est convenablement exploité. Même si ce n'est pas le cas, un pirate peut utiliser ce bogue pour accéder à un compte local sans privilège, afin d'exploiter les autres faiblesses éventuelles du système.

Les dépassements de tampon et les bogues de chaîne de format sur une liaison réseau sont probablement les variantes les plus fréquentes d'attaques distantes en général. Les listes de diffusion sur la sécurité publient fréquemment des exploits, programmes qui permettent d'exploiter ces nouvelles failles de sécurité. Ils permettent de cibler la faiblesse sans connaître les détails du code. L'expérience a montré que la libre disposition des codes d'exploit a permis d'améliorer la sécurité des systèmes d'exploitation, puisque les fabricants de systèmes d'exploitation ont été obligés de régler les problèmes de leurs logiciels. Avec les logiciels libres, tout le monde a accès au code source (SUSE Linux est fourni avec tous les codes source disponibles), et toute personne qui découvre une faiblesse et son code d'exploit peut proposer un correctif pour réparer le bogue en question.

Déni de service

Le but d'une attaque par déni de service est de bloquer le programme d'un serveur, voire un système entier. Ce type d'attaque s'effectue de plusieurs manières : en surchargeant le serveur, en l'occupant avec des paquets de données inutiles ou en exploitant un dépassement de tampon à distance. Souvent, l'attaque par déni de service vise exclusivement à faire disparaître le service. Toutefois, une fois qu'un service est indis-

ponible, les communications peuvent devenir vulnérables vis-à-vis des *attaques de l'intercepteur* (reniflage de paquets, détournement de connexions TCP, usurpation d'identité) et de l'empoisonnement DNS.

Attaques de l'intercepteur : reniflage, détournement, usurpation

En règle générale, toute attaque perpétrée à distance par un pirate informatique qui se place entre les hôtes en communication porte le nom d'*attaque de l'intercepteur*. Dans la quasi-totalité de ces attaques, la victime n'est généralement pas consciente de la situation. Il existe de nombreuses variantes. Par exemple, le pirate peut récupérer une requête de connexion et la transmettre à la machine cible. La victime a donc, sans le savoir, établi une connexion avec le mauvais hôte, parce que ce dernier s'identifie comme étant la cible légitime.

La forme d'attaque de l'intercepteur la plus simple porte le nom de *reniflage de paquets (sniffer)* : le pirate épie « simplement » le trafic réseau. Dans le cadre d'une attaque plus complexe, l'« intercepteur » peut essayer de prendre possession d'une connexion déjà établie (détournement). Pour ce faire, le pirate doit analyser les paquets pendant un certain temps, afin de pouvoir prédire les numéros de séquence TCP de la connexion. Lorsqu'il prend le rôle de l'hôte cible, la victime le remarque, puisqu'elle reçoit un message d'erreur qui indique que la connexion a été interrompue en raison d'une défaillance. Il existe des protocoles non protégés contre le détournement par codage, qui ne suivent qu'une simple procédure d'authentification lors de la connexion, ce qui facilite le travail des pirates.

L'*usurpation* est une attaque qui consiste à modifier les paquets pour qu'ils contiennent des données source falsifiées (généralement l'adresse IP). Les formes d'attaque les plus actives consistent à envoyer ces paquets falsifiés, tâche que seul le superutilisateur (utilisateur `root`) peut effectuer sous Linux.

La plupart des attaques mentionnées ci-dessus sont perpétrées en combinaison avec une attaque par déni de service. Si le pirate a la possibilité d'interrompre brusquement un certain hôte, même pour une courte durée, il pourra perpétrer plus facilement son attaque, puisque l'hôte ne sera pas en mesure de la contrer pendant ce délai.

Empoisonnement DNS

L'empoisonnement DNS signifie que le pirate corrompt le cache d'un serveur DNS en lui répondant avec des paquets de réponses DNS falsifiés. Il tente ainsi de faire en sorte que le serveur envoie certaines données à la victime qui demande des informations à ce serveur. La plupart des serveurs maintiennent une relation de confiance avec les autres hôtes, basée sur les adresses IP ou les noms d'hôte. Le pirate doit avoir une bonne connaissance de la structure réelle de cette relation de confiance entre les hôtes, afin de se faire lui-même passer pour un hôte digne de confiance. Généralement, il analyse certains paquets reçus du serveur, afin d'obtenir les informations nécessaires. Pour le pirate, il est souvent nécessaire de programmer également une attaque par déni de service opportune contre le serveur de noms. Pour vous protéger, utilisez des connexions codées qui sont capables de vérifier l'identité des hôtes auxquels vous vous connectez.

Les vers

On confond souvent les vers et les virus, mais il existe une différence évidente entre les deux. Contrairement aux virus, les vers n'ont pas besoin d'infecter un programme hôte pour vivre. En revanche, ils ont pour caractéristique de se propager le plus rapidement possible sur des structures réseau. Les vers apparus dans le passé, tels que Ramen, Lion ou Adore, utilisent les brèches de sécurité connues de programmes serveur comme bind8 ou lprNG. La protection contre les vers est relativement simple. Un certain laps de temps s'écoule entre la découverte d'une faille de sécurité et le moment où le ver s'attaque à votre serveur. Par conséquent, vous avez généralement le temps de vous procurer la version à jour du programme en question. L'administrateur doit toutefois installer les mises à jour de sécurité sur le système concerné.

23.4.2 Conseils et astuces en matière de sécurité

Pour assurer efficacement la sécurité, vous devez suivre l'évolution des produits et être au fait des derniers problèmes de sécurité. L'un des meilleurs moyens de protéger vos systèmes contre les problèmes de toutes sortes consiste à vous procurer et à installer le plus rapidement possible les paquetages mis à jour et recommandés par les annonces sur la sécurité. Les annonces de sécurité de SUSE sont publiées sur une liste de diffusion. Pour vous y inscrire, cliquez sur le lien suivant : `http://www.novell.com/linux/security/securitysupport.html`. La liste

suse-security-announce@suse.de est une source d'informations de première main sur les paquetages mis à jour. Les membres de l'équipe de sécurité de SUSE comptent parmi ses collaborateurs les plus actifs.

La liste de diffusion suse-security@suse.de est le lieu idéal pour discuter des principaux problèmes de sécurité. Vous pouvez vous y inscrire sur la même page Web.

L'une des listes de diffusion les plus connues au monde en matière de sécurité est la liste bugtraq@securityfocus.com. Nous vous recommandons de vous abonner à cette liste de diffusion, qui reçoit entre 15 et 20 messages par jour. Pour en savoir plus, consultez le site http://www.securityfocus.com.

Voici quelques règles utiles en matière de sécurité :

- Conformément à la règle préconisant d'utiliser l'ensemble d'autorisations le plus limité pour chaque tâche, évitez d'effectuer les tâches classiques en tant qu'utilisateur `root`. En plus de vous protéger contre vos propres erreurs, vous limiterez ainsi le risque d'oeuf de coucou et de contamination par un virus.

- Si possible, essayez d'utiliser systématiquement des connexions codées pour travailler sur une machine distante. Il est recommandé d'utiliser `ssh` (shell sécurisé) à la place de `telnet`, `ftp`, `rsh` et `rlogin`.

- Évitez d'utiliser des méthodes d'authentification basées sur les adresses IP uniquement.

- Essayez de mettre à jour régulièrement les paquetages réseau les plus importants et inscrivez-vous aux listes de diffusion correspondantes pour recevoir les annonces sur les nouvelles versions de ces programmes (bind, sendmail, ssh, etc.). Le même principe s'applique pour les logiciels relatifs à la sécurité locale.

- Modifiez le fichier `/etc/permissions` pour optimiser les autorisations des fichiers indispensables à la sécurité de votre système. Si vous supprimez le bit setuid d'un programme, il ne pourra sans doute plus remplir sa fonction correctement. En revanche, le programme ne représentera plus un risque de sécurité potentiel. Vous pouvez utiliser le même processus pour les fichiers et les répertoires pour lesquels tout utilisateur possède des droits en écriture.

- Désactivez tous les services réseau dont vous n'avez pas absolument besoin pour que votre serveur fonctionne correctement. Votre système sera ainsi plus sûr. Utilisez le programme netstat pour identifier les ports ouverts (ceux dont l'état est LISTEN).

Comme pour les options, nous vous recommandons d'utiliser `netstat -ap` ou `netstat -anp`. L'option `-p` vous permet d'identifier quel processus occupe quel port et sous quel nom.

Comparez les résultats donnés par netstat et ceux d'une analyse approfondie des ports effectuée par un élément extérieur à votre hôte. Pour ce faire, vous pouvez utiliser l'excellent programme nmap, qui contrôle les ports de votre machine et en tire des conclusions au sujet des services en attente derrière ces ports. Toutefois, l'analyse des ports pouvant être interprétée comme un acte agressif, nous vous recommandons de demander l'autorisation expresse de l'administrateur avant de l'effectuer sur un hôte. Enfin, n'oubliez pas qu'il est important d'analyser les ports TCP, mais également les ports UDP (options `-sS` et `-sU`).

- Pour surveiller l'intégrité des fichiers de votre système de façon fiable, utilisez le programme AIDE (Advanced Intrusion Detection Environment), disponible sur SUSE Linux. Codez la base de données créée par AIDE pour éviter que quelqu'un ne la falsifie. En outre, conservez une sauvegarde de cette base de données en dehors de votre machine, stockée sur un support de données externe non connecté à l'ordinateur par une liaison réseau.

- Prenez toutes les précautions nécessaires lorsque vous installez un logiciel tiers. Il est déjà arrivé qu'un pirate intègre un cheval de Troie dans l'archive tar d'un logiciel de sécurité. Heureusement, il avait été rapidement détecté. Si vous installez un paquetage binaire, vous devez être sûr de sa provenance.

  Les paquetages RPM de SUSE comportent une signature gpg. Pour signer, SUSE utilise la clé suivante :

  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

  Empreinte de la clé = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

  La commande `rpm --checksig package.rpm` indique si la somme de contrôle et la signature d'un paquetage désinstallé sont correctes. Vous trouverez la clé sur le premier CD de la distribution et sur les principaux serveurs de clés existants.

- Vérifiez régulièrement les sauvegardes de vos fichiers système et utilisateur. Rappelez-vous que si vous ne testez pas le fonctionnement de votre sauvegarde, elle peut être totalement inutile.

- Vérifiez vos fichiers journaux. Si vous le pouvez, écrivez un petit script pour rechercher les entrées suspectes dans vos fichiers journaux. Il est vrai que cette tâche n'est pas évidente. Au final, vous seul pouvez déterminer les entrées inhabituelles et celles qui ne le sont pas.

- Utilisez `tcp_wrapper` pour restreindre l'accès à chaque service exécuté sur votre machine. Vous disposez ainsi d'un contrôle explicite pour déterminer les adresses IP qui peuvent se connecter à un service. Pour plus d'informations sur `tcp_wrapper`, consultez les pages du manuel de tcpd et hosts_access (`man 8 tcpd`, `man hosts_access`).

- Utilisez SuSEfirewall pour optimiser la sécurité offerte par tcpd (tcp_wrapper).

- N'hésitez pas à être répétitif lorsque vous élaborez vos mesures de sécurité : un message en double est largement préférable à un message qui n'apparaît pas du tout.

23.4.3 Notification centralisée des problèmes de sécurité

Si vous découvrez un problème de sécurité (vérifiez d'abord les paquetages de mise à jour disponibles), envoyez un message électronique à `security@suse.de`. N'oubliez pas de joindre une description détaillée du problème, ainsi que le numéro de version du paquetage concerné. SUSE vous répondra le plus rapidement possible. Nous vous recommandons de coder vos messages électroniques avec la technologie pgp. La clé pgp de SUSE est la suivante :

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Vous pouvez également télécharger cette clé sur le site `http://www.novell.com/linux/security/securitysupport.html`.

Listes de contrôle d'accès sous Linux 24

Ce chapitre fournit un résumé rapide des bases et des fonctions des ACL (access control list - liste de contrôle d'accès) POSIX pour systèmes de fichiers Linux. Les ACL peuvent être utilisées comme une extension du concept traditionnel d'autorisation pour les objets Système de fichiers. Les ACL permettent de définir des autorisations plus facilement que le concept d'autorisation traditionnel.

L'expression *ACL POSIX* laisse entendre qu'il s'agit d'une norme POSIX (*interface de système d'exploitation portable*) à proprement parler. Les normes en projet POSIX 1003.1e et POSIX 1003.2c ont été retirées pour plusieurs raisons. Néanmoins, les ACL telles qu'on les trouve sur de nombreux systèmes appartenant à la famille UNIX sont basées sur ces projets et l'implémentation des ACL de système de fichiers décrites dans ce chapitre suit également ces deux normes. Vous pouvez les consulter à l'adresse `http://wt.xpilot.org/publications/posix.1e/`.

24.1 Avantages des ACL

Généralement, trois ensembles d'autorisations sont définis pour chaque objet Fichier sur un système Linux. Ces ensembles comprennent les autorisations de lecture (`r`), d'écriture (`w`) et d'exécution (`x`) pour chacun des trois types d'utilisateurs : le propriétaire du fichier, le groupe et les autres utilisateurs. En outre, il est possible de définir les bits *set user id*, *set group id* et *sticky*. Ce concept simple est parfaitement adapté dans la plupart des cas pratiques. Cependant, pour les scénarios plus complexes ou les applications avancées, les administrateurs système devaient auparavant utiliser un certain nombre d'astuces pour contourner les limitations du concept d'autorisation traditionnel.

Les ACL peuvent être utilisées dans les situations nécessitant une extension du concept d'autorisation de fichier traditionnel. Elles permettent l'assignation d'autorisations à des utilisateurs ou à des groupes particuliers, même si ceux-ci ne correspondent pas au propriétaire d'origine ou au groupe propriétaire. Les listes de contrôle d'accès sont une fonctionnalité du kernel Linux et sont actuellement prises en charge par ReiserFS, Ext2, Ext3, JFS et XFS. Les ACL permettent de réaliser des scénarios complexes sans implémenter des modèles d'autorisation complexes au niveau de l'application.

Les avantages des ACL sont évidents dans certaines situations, comme le remplacement d'un serveur Windows par un serveur Linux. Certains des postes de travail connectés peuvent continuer à fonctionner sous Windows même après la migration. Le système Linux offre des services de fichier et d'impression aux clients Windows à l'aide de Samba. Étant donné que Samba prend en charge les listes de contrôle d'accès, les autorisations utilisateur peuvent être configurées sur le serveur Linux et sous Windows avec une interface utilisateur graphique (uniquement sous Windows NT et versions ultérieures). winbindd permet même d'assigner des autorisations aux utilisateurs qui existent uniquement dans le domaine Windows sans compte sur le serveur Linux.

24.2 Définitions

classe d'utilisateur

Le concept conventionnel d'autorisation POSIX utilise trois *classes* d'utilisateurs pour l'assignation des autorisations dans le système de fichiers : le propriétaire, le groupe propriétaire et les autres utilisateurs. Trois bits d'autorisation peuvent être définis pour chaque classe d'utilisateur : en lecture (`r`), en écriture (`w`) et en exécution (`x`).

ACL d'accès

Les autorisations d'accès de l'utilisateur et du groupe pour tous les types d'objets Système de fichiers (fichiers et répertoires) sont déterminées au moyen des ACL d'accès.

ACL par défaut

Les ACL par défaut s'appliquent uniquement aux répertoires. Elles déterminent les autorisations qu'un objet Système de fichiers hérite de son répertoire parent lors de sa création.

entrée ACL

Chaque ACL est composée d'un ensemble d'entrées ACL. Une entrée ACL contient un type (consultez le Tableau 24.1, « Types d'entrées ACL » (p. 380)), un qualificateur de l'utilisateur ou du groupe auquel l'entrée se rapporte et un ensemble d'autorisations. Pour certains types d'entrées, le qualificateur du groupe ou des utilisateurs n'est pas défini.

24.3 Gestion des ACL

Le Tableau 24.1, « Types d'entrées ACL » (p. 380) présente les six types possibles d'entrées ACL, chacun définissant les autorisations d'un utilisateur ou d'un groupe d'utilisateurs. L'entrée *propriétaire* définit les autorisations de l'utilisateur propriétaire du fichier ou du répertoire. L'entrée *groupe propriétaire* définit les autorisations du groupe propriétaire du fichier. Le superutilisateur peut modifier le propriétaire ou le groupe propriétaire via l'une des commandes `chown` ou `chgrp`. Dans ce cas, les entrées du propriétaire et du groupe propriétaire font référence au nouveau propriétaire et au nouveau groupe propriétaire. Chaque entrée *utilisateur nommé* définit les autorisations de l'utilisateur spécifié dans le champ de qualification de l'entrée, à savoir le champ du milieu, au format texte, représenté dans le Tableau 24.1, « Types d'entrées ACL » (p. 380). Chaque entrée *groupe nommé* définit les autorisations du groupe spécifié dans le champ de qualification de l'entrée. Seules les entrées d'utilisateur nommé et de groupe nommé disposent d'un champ de qualification qui n'est pas vide. L'entrée *autre* définit les autorisations de tous les autres utilisateurs.

L'entrée *masque* limite davantage les autorisations accordées par les entrées *utilisateur nommé*, *groupe nommé* et *groupe propriétaire* en définissant, parmi ces entrées, les autorisations qui sont en vigueur et celles qui sont masquées. Si des autorisations sont paramétrées dans l'une des entrées mentionnées ainsi que dans le masque, elles sont en vigueur. Les autorisations contenues uniquement dans le masque ou uniquement dans l'entrée à proprement parler ne sont pas en vigueur, c'est-à-dire qu'elles ne sont pas accordées. Toutes les autorisations définies dans les entrées *propriétaire* et *groupe propriétaire* sont toujours en vigueur. L'exemple du Tableau 24.2, « Masquage des autorisations d'accès » (p. 380) illustre ce mécanisme.

Il existe deux classes basiques d'ACL : une ACL *minimum* contient uniquement les entrées des types *propriétaire*, *groupe propriétaire* et *autre*, qui correspondent aux bits conventionnels d'autorisation pour les fichiers et les répertoires. Une ACL *étendue* va

plus loin. Elle doit contenir une entrée *masque* et peut contenir plusieurs entrées de type *utilisateur nommé* et *groupe nommé*.

Tableau 24.1 *Types d'entrées ACL*

Type	Forme textuelle
propriétaire	`user::rwx`
utilisateur nommé	`user:name:rwx`
groupe propriétaire	`group::rwx`
groupe nommé	`group:name:rwx`
masque	`mask::rwx`
autre	`other::rwx`

Tableau 24.2 *Masquage des autorisations d'accès*

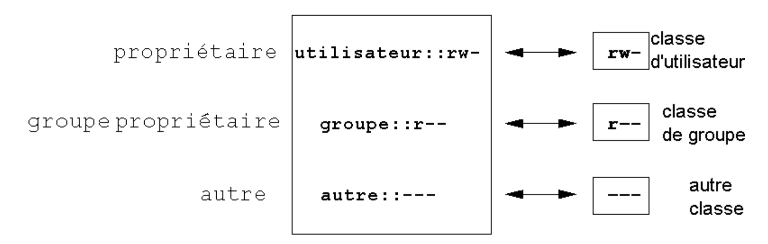
Type d'entrée	Forme textuelle	Autorisations
utilisateur nommé	`user:geeko:r-x`	`r-x`
masque	`mask::rw-`	`rw-`
	autorisations en vigueur :	`r--`

24.3.1 Entrées ACL et bits d'autorisation en mode fichier

La Figure 24.1, « ACL minimum : Entrées ACL comparées aux bits d'autorisation » (p. 381) et la Figure 24.2, « ACL étendue : Entrées ACL comparées aux bits d'autorisation » (p. 381) illustrent les deux cas d'ACL minimum et d'ACL étendue. Les figures sont structurées en trois blocs : le bloc de gauche représente les spécifications de type des entrées ACL, le bloc central affiche un exemple d'ACL et le bloc de droite

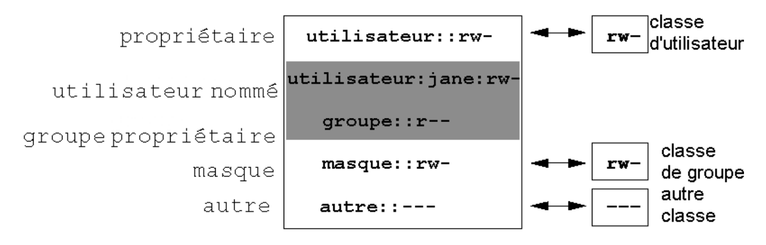
représente les bits d'autorisation correspondants selon le concept d'autorisation conventionnel, par exemple, tel qu'ils sont affichés par la commande `ls -l`. Dans les deux cas, les autorisations de la *classe propriétaire* sont assignées à l'entrée ACL *propriétaire*. Les autorisations *Autre classe* sont assignées à l'entrée ACL correspondante. Cependant, l'assignation des autorisations *classe de groupe* est différente dans les deux cas.

Figure 24.1 *ACL minimum : Entrées ACL comparées aux bits d'autorisation*



Dans le cas d'une ACL minimum, sans *masque*, les autorisations de la *classe de groupe* sont assignées à l'entrée ACL *groupe propriétaire*. Consultez la Figure 24.1, « ACL minimum : Entrées ACL comparées aux bits d'autorisation » (p. 381). Dans le cas d'une ACL étendue, avec *masque*, les autorisations de la *classe de groupe* sont assignées à l'entrée *masque*. Consultez la Figure 24.2, « ACL étendue : Entrées ACL comparées aux bits d'autorisation » (p. 381).

Figure 24.2 *ACL étendue : Entrées ACL comparées aux bits d'autorisation*



Cette approche d'assignation garantit l'interaction régulière des applications, qu'elles prennent en charge les ACL ou non. Les autorisations d'accès qui ont été assignées au moyen des bits d'autorisation représentent la limite supérieure de tous les autres « paramétrages avancés » effectués avec une ACL. Les modifications apportées aux bits d'autorisation sont reflétées par l'ACL et inversement.

24.3.2 Répertoire avec une ACL d'accès

La gestion des ACL d'accès est présentée dans l'exemple suivant :

Avant de créer le répertoire, utilisez la commande `umask` pour définir les autorisations d'accès qui doivent être masquées chaque fois qu'un objet Fichier est créé. La commande `umask 027` définit les autorisations par défaut en donnant au propriétaire toute la plage d'autorisations (`0`), en refusant au groupe l'accès en écriture (`2`) et en ne donnant aucune autorisation aux autres utilisateurs (`7`). En fait, `umask` masque les bits d'autorisation correspondants ou les désactive. Pour plus d'informations, consultez la page du manuel correspondante (`man umask`).

`mkdir monrép` doit créer le répertoire `monrép` avec les autorisations par défaut telles qu'elles sont définies par `umask`. Utilisez `ls -dl monrép` pour vérifier si toutes les permissions ont été assignées correctement. Voici la sortie de cet exemple :

```
drwxr-x--- ... tux projet3 ... monrép
```

Avec `getfacl monrép`, vérifiez l'état initial de l'ACL. Vous obtenez des informations telles que :

```
# file: monrép
# owner: tux
# group: projet3
user::rwx
group::r-x
other::---
```

La sortie de `getfacl` reflète précisément l'assignation des bits d'autorisation et les entrées ACL décrites à la Section 24.3.1, « Entrées ACL et bits d'autorisation en mode fichier » (p. 380). Les trois premières lignes de sortie affichent le nom, le propriétaire et le groupe propriétaire du répertoire. Les trois lignes suivantes contiennent les trois entrées ACL *propriétaire*, *groupe propriétaire* et *autre*. En fait, dans le cas de l'ACL minimum, la commande `getfacl` ne génère pas plus d'informations que la commande `ls`.

Modifiez l'ACL pour assigner des autorisations en lecture, écriture et exécution à l'utilisateur supplémentaire `geeko` et au groupe supplémentaire `mascots`, comme suit :

```
setfacl -m user:geeko:rwx,group:mascots:rwx monrép
```

L'option `-m` demande à `setfacl` de modifier l'ACL existante. L'argument suivant désigne les entrées ACL à modifier (des entrées multiples sont séparées par des virgules). La partie finale indique le nom du répertoire dans lequel ces modifications doivent être appliquées. Utilisez la commande `getfacl` pour consulter l'ACL obtenue.

```
# file: monrép
# owner: tux
# group: projet3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

En plus des entrées lancées pour l'utilisateur `geeko` et le groupe `mascots`, une entrée *mask* a été générée. Cette entrée *mask* est définie automatiquement afin que toutes les autorisations entrent en vigueur. `setfacl` adapte automatiquement les entrées *mask* aux paramètres modifiés à moins que vous ne désactiviez cette fonctionnalité avec `-n`. *mask* définit les autorisations d'accès maximum en vigueur pour toutes les entrées de la *classe de groupe*, notamment l'*utilisateur nommé*, le *groupe nommé* et le *groupe propriétaire*. Les bits d'autorisation de la *classe de groupe* affichés via `ls -dl monrép` correspondent maintenant à l'entrée `mask`.

```
drwxrwx---+ ... tux projet3 ... monrép
```

La première colonne de la sortie contient désormais un signe + qui indique que cet élément possède une ACL *étendue*.

En fonction de la sortie de la commande `ls`, les autorisations de l'entrée *mask* comprennent l'accès en écriture. Généralement, de tels bits d'autorisation signifient que le *groupe propriétaire* (ici `projet3`) dispose également d'un accès en écriture au répertoire `monrép`. Cependant, les autorisations d'accès en vigueur du *groupe propriétaire* correspondent à la partie commune avec les autorisations définies pour le *groupe propriétaire* et le *masque* (`r-x` dans notre exemple) (consultez le Tableau 24.2, « Masquage des autorisations d'accès » (p. 380)). En ce qui concerne les autorisations en vigueur du *groupe propriétaire* de cet exemple, rien n'a été modifié même après l'ajout des entrées ACL.

Modifiez l'entrée du *masque* avec `setfacl` ou `chmod`. Par exemple, utilisez `chmod g-w monrép`. `ls -dl monrép` affiche ensuite :

```
drwxr-x---+ ... tux projet3 ... monrép
```

`getfacl monrép` génère la sortie suivante :

```
# file: monrép
# owner: tux
# group: projet3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx      # effective: r-x
mask::r-x
other::---
```

Une fois que vous avez exécuté la commande `chmod` pour supprimer l'autorisation en écriture des bits de la *classe de groupe*, la sortie de la commande `ls` suffit pour voir que les bits de *masque* doivent être modifiés en conséquence : l'autorisation en écriture est à nouveau limitée au propriétaire de `monrép`. La sortie de `getfacl` confirme ce fait. Cette sortie comprend un commentaire pour toutes les entrées dans lesquelles les bits d'autorisation en vigueur ne correspondent pas aux autorisations d'origine, car elles sont filtrées en fonction de l'entrée de *masque*. Les autorisations d'origine peuvent être restaurées à tout moment avec `chmod g+w monrép`.

24.3.3 Répertoire avec une ACL par défaut

Les répertoires peuvent avoir une ACL par défaut, type spécial d'ACL qui définit les autorisations d'accès dont les objets du répertoire héritent lors de leur création. Une ACL par défaut a un effet sur les sous-répertoires et les fichiers.

Effets d'une ACL par défaut

Il existe deux manières de transmettre les autorisations d'une ACL par défaut d'un répertoire aux fichiers et aux sous-répertoires qu'il contient :

- Un sous-répertoire hérite de l'ACL par défaut du répertoire parent en tant qu'ACL par défaut et ACL d'accès.
- Un fichier hérite d'une ACL par défaut en tant qu'ACL d'accès.

Tous les appels système qui créent des objets Système de fichiers utilisent un paramètre `mode` qui définit les autorisations d'accès pour le nouvel objet Système de fichiers. Si le répertoire parent ne dispose pas d'une ACL par défaut, les bits d'autorisation définis par `umask` sont soustraits des autorisations transmises par le paramètre `mode`, le

résultat étant assigné au nouvel objet. Si le répertoire parent possède une ACL par défaut, les bits d'autorisation assignés au nouvel objet correspondent à la partie commune des autorisations du paramètre `mode` et à celles définies dans l'ACL par défaut. `umask` est ignoré dans ce cas.

Application des ACL par défaut

Les trois exemples suivants présentent les principales opérations des répertoires et des ACL par défaut :

1. Ajoutez une ACL par défaut au répertoire existant `monrép` à l'aide de :

   ```
   setfacl -d -m group:mascots:r-x monrép
   ```

   L'option `-d` de la commande `setfacl` demande à `setfacl` d'apporter les modifications suivantes (option `-m`) à l'ACL par défaut.

   Regardez plus attentivement le résultat de cette commande :

   ```
   getfacl monrép

   # file: monrép
   # owner: tux
   # group: projet3
   user::rwx
   user:geeko:rwx
   group::r-x
   group:mascots:rwx
   mask::rwx
   other::---
   default:user::rwx
   default:group::r-x
   default:group:mascots:r-x
   default:mask::r-x
   default:other::---
   ```

   `getfacl` retourne l'ACL d'accès et l'ACL par défaut. L'ACL par défaut est constituée de toutes les lignes commençant par `default`. Bien que vous ayez simplement exécuté la commande `setfacl` avec une entrée pour le groupe `mascots` de l'ACL par défaut, `setfacl` a automatiquement copié toutes les autres entrées de l'ACL d'accès pour créer une ACL par défaut valide. Les ACL par défaut n'ont pas d'effet immédiat sur les autorisations d'accès. Elles entrent uniquement en jeu lorsque des objets Système de fichiers sont créés. Ces nouveaux objets héritent des autorisations provenant uniquement de l'ACL par défaut de leur répertoire parent.

2. Dans l'exemple suivant, utilisez `mkdir` pour créer dans `monrép` un sous-répertoire qui hérite de l'ACL par défaut.

   ```
   mkdir monrép/monsousrép
   ```

   ```
   getfacl monrép/monsousrép
   ```

   ```
   # file: monrép/monsousrép
   # owner: tux
   # group: projet3
   user::rwx
   group::r-x
   group:mascots:r-x
   mask::r-x
   other::---
   default:user::rwx
   default:group::r-x
   default:group:mascots:r-x
   default:mask::r-x
   default:other::---
   ```

   Comme prévu, le nouveau répertoire `monsousrép` dispose des autorisations de l'ACL par défaut du répertoire parent. L'ACL d'accès de `monsousrép` est le reflet exact de l'ACL par défaut de `monrép`. L'ACL par défaut que ce répertoire doit transmettre à ses objets subordonnés est également identique.

3. Utilisez `touch` pour créer un fichier dans le répertoire `monrép`, par exemple, `touch monrép/monfichier`. `ls -l monrép/monfichier` affiche ensuite :

   ```
   -rw-r-----+ ... tux projet3 ... monrép/monfichier
   ```

   La sortie de `getfacl monrép/monfichier` est la suivante :

   ```
   # file: monrép/monfichier
   # owner: tux
   # group: projet3
   user::rw-
   group::r-x          # effective:r--
   group:mascots:r-x   # effective:r--
   mask::r--
   other::---
   ```

   `touch` utilise un paramètre `mode` avec la valeur `0666` lors de la création de fichiers, c'est-à-dire que les fichiers sont créés avec des autorisations en lecture/écriture pour toutes les classes d'utilisateurs, à condition qu'il n'existe aucune autre restriction dans `umask` ou dans l'ACL par défaut (consultez la section intitulée « Effets d'une ACL par défaut » (p. 384)). Autrement dit, toutes les

autorisations d'accès qui ne sont pas contenues dans la valeur `mode` sont supprimées des entrées ACL correspondantes. Bien qu'aucune autorisation n'ait été supprimée de l'entrée ACL de la *classe de groupe*, l'entrée de *masque* a été modifiée en autorisations de masque non définies dans le paramètre `mode`.

Cette approche garantit l'interaction correcte des applications, notamment des compilateurs, avec les ACL. Vous pouvez créer des fichiers avec des autorisations d'accès limitées et les marquer ultérieurement comme exécutables. Le mécanisme de `masque` garantit que les utilisateurs et les groupes corrects peuvent les exécuter selon leurs besoins.

24.3.4 Algorithme de contrôle des ACL

Un algorithme de contrôle est appliqué avant qu'un processus ou une application n'obtienne l'accès à un objet Système de fichiers protégé par ACL. En règle générale, les entrées ACL sont examinées dans l'ordre suivant : *propriétaire*, *utilisateur nommé*, *groupe propriétaire* ou *groupe nommé* et *autre*. L'accès est géré conformément à l'entrée qui correspond le mieux au processus. Les autorisations ne se cumulent pas.

Les choses sont plus compliquées si un processus appartient à plusieurs groupes et risque d'être adapté à plusieurs entrées de *groupe*. Une entrée est aléatoirement sélectionnée dans les entrées adaptées avec les autorisations nécessaires. Peu importe l'entrée qui déclenche le résultat final « accès accordé ». De même, si aucune des entrées adaptées du *groupe* ne contient les autorisations nécessaires, une entrée sélectionnée de manière aléatoire déclenche le résultat final « accès refusé ».

24.4 Prise en charge des ACL dans les applications

Les ACL peuvent être utilisées pour implémenter des scénarios d'autorisation très complexes qui répondent aux contraintes des applications modernes. Le concept d'autorisation traditionnel et les ACL peuvent se combiner intelligemment. À l'instar de Samba, les commandes basiques de fichier (`cp`, `mv`, `ls`, etc.) prennent en charge les ACL.

Malheureusement, de nombreux éditeurs et gestionnaires de fichiers ne prennent toujours pas en charge les ACL. Lorsque vous copiez des fichiers avec Konqueror, par exemple, les ACL de ces fichiers sont perdues. Lorsque vous modifiez des fichiers avec un éditeur, les ACL des fichiers sont parfois conservées, mais pas systématiquement, en fonction du mode de sauvegarde de l'éditeur utilisé. Si l'éditeur écrit les modifications dans le fichier d'origine, l'ACL d'accès est conservée. Si l'éditeur enregistre le contenu mis à jour dans un nouveau fichier qui est ensuite renommé avec l'ancien nom de fichier, les ACL risquent d'être perdues, sauf si l'éditeur prend en charge les ACL. Exception faite du programme d'archivage star, il n'existe actuellement aucune application de sauvegarde qui conserve les ACL.

24.5 Pour plus d'informations

Des informations détaillées sur les ACL sont disponibles sur le site `http://acl.bestbits.at/`. Consultez également les pages du manuel sur `getfacl(1)`, `acl(5)` et `setfacl(1)`.

25 Utilitaires de surveillance du système

Vous pouvez utiliser un certain nombre de programmes et de mécanismes, dont certains sont décrits ici, pour surveiller l'état de votre système. Ce chapitre contient également la description de certains utilitaires pratiques pour votre travail quotidien, ainsi que leurs principaux paramètres.

Pour chacune des commandes présentées, vous trouverez des exemples de sortie. Dans ces exemples, la première ligne contient la commande proprement dite (après le signe dollar de l'invite). Les commentaires sont indiqués par des crochets (`[...]`) et les lignes trop longues sont coupées si nécessaire. Les sauts de ligne insérés dans les lignes longues sont indiqués par une barre oblique inverse (\).

```
$ command -x -y
sortie ligne 1
sortie ligne 2
sortie ligne 3 est très longue, si bien \
  que nous devons insérer un retour
sortie ligne 4
[...]
sortie ligne 98
sortie ligne 99
```

Les descriptions sont très courtes pour permettre de citer autant d'utilitaires que possible. Des informations complémentaires sur toutes les commandes sont accessibles dans les pages de manuel. En outre, presque toutes les commandes acceptent le paramètre `--help`, qui génère une courte liste des paramètres possibles.

25.1 Liste des fichiers ouverts : lsof

Pour afficher la liste de tous les fichiers ouverts au cours du processus dont l'ID est *PID*, utilisez -p. Par exemple, pour afficher tous les fichiers utilisés par le shell actuel, entrez :

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t
(totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610
/usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410
/usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393
/usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565
/usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598
/usr/lib/zsh/4.2.0/zsh/computil.so
zsh     4694   jj    0u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48               50 /dev/pts/48
```

La variable de shell spéciale `$$`, dont la valeur correspond à l'ID de processus du shell, a été utilisée.

La commande `lsof` répertorie tous les fichiers actuellement ouverts lorsqu'elle est utilisée sans aucun paramètre. Comme il y a souvent des milliers de fichiers ouverts, il est rarement utile de tous les répertorier. Cependant, il est possible de combiner la liste de tous les fichiers avec des fonctions de recherche, afin de générer des listes utiles. Par exemple, vous pouvez répertorier tous les périphériques en mode caractères utilisés :

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
```

```
sshd        4693      jj  mem    CHR    1,5             45833 /dev/zero
sshd        4693      jj  mem    CHR    1,5             45833 /dev/zero
zsh         4694      jj    0u   CHR 136,48                50 /dev/pts/48
zsh         4694      jj    1u   CHR 136,48                50 /dev/pts/48
zsh         4694      jj    2u   CHR 136,48                50 /dev/pts/48
zsh         4694      jj   10u   CHR 136,48                50 /dev/pts/48
X           6476    root  mem    CHR    1,1             38042 /dev/mem
lsof       13478      jj    0u   CHR 136,48                50 /dev/pts/48
lsof       13478      jj    2u   CHR 136,48                50 /dev/pts/48
grep       13480      jj    1u   CHR 136,48                50 /dev/pts/48
grep       13480      jj    2u   CHR 136,48                50 /dev/pts/48
```

25.2 Utilisateur qui accède aux fichiers : fuser

Il peut être utile de déterminer les processus ou les utilisateurs qui accèdent actuellement à certains fichiers. Supposons, par exemple, que vous souhaitiez démonter un système de fichiers monté sous /mnt. La commande umount signale que le périphérique est occupé. Vous pouvez employer la commande fuser pour déterminer les processus qui accèdent au périphérique :

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

A la fin du processus less, qui s'exécutait sur un autre terminal, le système de fichiers peut être démonté.

25.3 Propriétés d'un fichier : stat

La commande stat affiche les propriétés d'un fichier :

```
$ stat xml-doc.txt
  File: `xml-doc.txt'
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
```

```
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Le paramètre `--filesystem` fournit des détails sur les propriétés du système de fichiers contenant le fichier spécifié :

```
 $ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388    Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Si vous utilisez le shell z (`zsh`), vous devez saisir `/usr/bin/stat`, car le shell z possède une commande shell intégrée, `stat`, dont les options et le format de sortie sont différents :

```
% type
stat stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

25.4 Périphériques USB : lsusb

La commande `lsusb` répertorie tous les périphériques USB. L'option `-v` permet d'afficher une liste plus détaillée. Les informations détaillées sont lues à partir du répertoire `/proc/bus/usb/`. Voici la sortie de la commande `lsusb` après connexion d'une clé USB. Les dernières lignes indiquent la présence du nouveau périphérique.

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

25.5 Informations relatives à un périphérique SCSI : scsiinfo

La commande `scsiinfo` affiche la liste des informations relatives à un périphérique SCSI. L'option `-l` répertorie tous les périphériques SCSI connus du système (similaire à la sortie de la commande `lsscsi`). Vous trouverez ci-dessous la sortie de la commande `scsiinfo -i /dev/sda`, qui affiche des informations sur un disque dur. L'option `-a` permet d'afficher encore plus d'informations.

```
Inquiry command
---------------
Relative Address                   0
Wide bus 32                        0
Wide bus 16                        1
Synchronous neg.                   1
Linked Commands                    1
Command Queueing                   1
SftRe                              0
Device Type                        0
Peripheral Qualifier               0
Removable?                         0
Device Type Modifier               0
ISO Version                        0
ECMA Version                       0
ANSI Version                       3
AENC                               0
TrmIOP                             0
Response Data Format               2
Vendor:                    FUJITSU
Product:                   MAS3367NP
Revision level:            0104A0K7P43002BE
```

Il existe une liste de défauts, avec deux tables qui indiquent les blocs défectueux d'un disque dur : la première est fournie par le fournisseur (table du fabricant) et la seconde répertorie les blocs défectueux qui apparaissent en cours de fonctionnement (table enrichie). Si le nombre d'entrée de la table enrichie augmente, il est conseillé de remplacer le disque dur.

25.6 Processus : top

La commande `top` (pour « Table of Processes » - table des processus) affiche la liste des processus, qui est rafraîchie toutes les deux secondes. Pour terminer le programme,

appuyez sur Q. Le paramètre `-n 1` termine le programme après un seul affichage de la liste des processus. Voici la sortie de la commande `top -n 1` :

```
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0   820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0   100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0     0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0     0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0     0    0    0 S  0.0  0.0   0:00.71 bdflush
       [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Si vous appuyez sur F pendant l'exécution de la commande `top`, vous voyez apparaître un menu qui vous permet de modifier très précisément le format de la sortie.

Le paramètre `-U UID` surveille uniquement les processus associés à un utilisateur particulier. Remplacez *`UID`* par l'ID utilisateur de l'utilisateur. La commande `top -U $(id -u username)` retourne l'UID de l'utilisateur en fonction de son nom (username) et affiche ses processus.

25.7 Liste des processus : ps

La commande `ps` génère la liste des processus. Si le paramètre `r` est ajouté, seuls les processus qui utilisent actuellement des ressources système sont affichés :

```
$ ps r
  PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

Ce paramètre doit être écrit sans signe moins. Les divers paramètres sont parfois écrits avec un signe moins, parfois sans. La page de manuel peut paraître complexe à l'utilisateur, mais la commande `ps --help` en génère une version abrégée.

Pour vérifier le nombre de processus `emacs` en cours d'exécution, utilisez :

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Le paramètre `-p` sélectionne les processus en fonction de l'ID processus :

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
  -B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
 4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      00:02:00 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

Vous pouvez formater la liste des processus en fonction de vos besoins. L'option `-L` retourne la liste de tous les mots-clés. Entrez la commande suivante pour générer la liste de tous les processus, triés en fonction de la quantité de mémoire qu'ils utilisent :

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
```

```
17010 5356 xterm
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth
/var/lib/xdm/authdir/au
```

25.8 Arborescence de processus : pstree

La commande `pstree` génère la liste des processus sous forme d'arborescence :

```
$ pstree
init-+-atd
     |-3*[automount]
     |-bdflush
     |-cron
  [...]
     |-usb-storage-1
     |-usb-storage-2
     |-10*[xterm---zsh]
     |-xterm---zsh---mutt
     |-2*[xterm---su---zsh]
     |-xterm---zsh---ssh
     |-xterm---zsh---pstree
     |-ypbind---ypbind---2*[ypbind]
     `-zsh---startx---xinit4-+-X
                             `-ctwm-+-xclock
                                    |-xload
                                    `-xosview.bin
```

Le paramètre `-p` ajoute l'ID processus au nom indiqué. Pour afficher aussi les lignes de commande, utilisez le paramètre `-a` :

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  `-zsh,1404
      `-startx,1407 /usr/X11R6/bin/startx
          `-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              `-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
                  |-xload,1450 -scale 2
                  `-xosview.bin,1451 +net -bat +net
```

25.9 Qui fait quoi : w

A l'aide de la commande `w`, vous pouvez savoir qui est logué au système et ce que fait chaque utilisateur. Par exemple :

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

La dernière ligne indique que l'utilisateur jj a établi une connexion shell (`ssh`) sécurisée avec l'ordinateur `totan`. Si des utilisateurs d'autres systèmes se sont logués à distance, le paramètre `-f` affiche les ordinateurs à partir desquels ils ont établi la connexion.

25.10 Utilisation de la mémoire : free

L'utilitaire `free` examine l'utilisation de la mémoire (RAM). Il affiche les détails de la quantité de mémoire libre et utilisée (ainsi que des zones d'échange) :

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Avec l'option `-m`, toutes les tailles sont exprimées en mégaoctets :

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

Les informations vraiment intéressantes se trouvent à la ligne suivante :

```
-/+ buffers/cache:        191        311
```

Cette ligne calcule la quantité de mémoire occupée par les tampons et les caches. Le paramètre `-d delay` assure le rafraîchissement de l'affichage à l'intervalle (en secondes) fixé par *`delay`*. Par exemple, `free -d 1.5` procède à une mise à jour toutes les 1,5 secondes.

25.11 Tampon circulaire du kernel : dmesg

Le kernel Linux conserve certains messages dans un tampon circulaire. Pour afficher ces messages, entrez la commande `dmesg`:

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

La dernière ligne indique un problème temporaire du serveur NFS `totan`. Les lignes qui précèdent sont générées par l'insertion d'un lecteur flash USB. Les événements plus anciens sont consignés dans les fichiers `/var/log/messages` et `/var/log/warn`.

25.12 Les systèmes de fichiers et leur utilisation : mount, df et du

La commande `mount` indique le système de fichiers (périphérique et type) qui est monté, ainsi que le point de montage correspondant :

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

Pour obtenir des informations sur l'utilisation totale des systèmes de fichiers, utilisez la commande `df`. Le paramètre `-h` (ou `--human-readable` (format lisible)) transforme la sortie en un texte compréhensible pour les utilisateurs.

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Les utilisateurs du serveur de fichiers NFS `totan` doivent effacer leur répertoire personnel le plus rapidement possible. Vous pouvez utiliser la commande `du` pour afficher la taille totale de tous les fichiers d'un répertoire donné et de ses sous-répertoires. Le paramètre `-s` supprime la sortie des informations détaillées. Là aussi, l'option `-h` affiche les données sous une forme compréhensible. Avec cette commande :

```
$ du -sh ~
361M    /suse/jj
```

vous pouvez savoir la quantité d'espace occupée par votre répertoire personnel.

25.13 Le système de fichiers /proc

Le système de fichiers `/proc` est un pseudo-système de fichiers, dans lequel le kernel stocke les informations importantes sous forme de fichiers virtuels. Par exemple, vous pouvez afficher le type du processeur, à l'aide de la commande suivante :

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

Vous pouvez également lancer une requête pour afficher l'allocation et l'utilisation des interruptions, avec la commande suivante :

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Voici la liste des fichiers important et des informations qu'ils contiennent :

`/proc/devices`
  périphériques disponibles

`/proc/modules`
  modules de kernel chargés

/proc/cmdline
ligne de commande du kernel

/proc/meminfo
informations détaillées sur l'utilisation de la mémoire

/proc/config.gz
`gzip` : fichier de configuration compressé du kernel en cours d'exécution

D'autres informations sont disponibles dans le fichier texte `/usr/src/linux/Documentation/filesystems/proc.txt`. Des informations sur les processus en cours d'exécution figurent dans les répertoires `/proc/` *NNN*, où *NNN* représente l'ID (PID) du processus concerné. Chaque processus trouve ses propres caractéristiques dans `/proc/self/` :

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

L'assignation d'adresse des fichiers exécutables et des bibliothèques figure dans le fichier `maps` :

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
```

```
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

25.14 Commandes vmstat, iostat et mpstat

L'utilitaire `vmstat` génère des statistiques sur la mémoire virtuelle. Il lit les fichiers `/proc/meminfo`, `/proc/stat` et `/proc/*/stat`. Cela est utile pour identifier les goulets d'étranglement au niveau des performances du système. La commande `iostat` génère des statistiques sur le processeur (CPU), ainsi que sur les entrées et sorties des périphériques et des partitions. Les informations affichées sont générées à partir des fichiers `/proc/stat` et `/proc/partitions`. La sortie peut servir à équilibrer la charge d'entrée et de sortie entre les différents disques durs. La commande `mpstat` génère des statistiques sur le processeur (CPU).

25.15 procinfo

La commande `procinfo` synthétise des informations importantes provenant du système de fichiers `/proc` :

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       02:42:28.08   1.3%  page in :        0
nice  :       00:31:57.13   0.2%  page out:        0
system:       00:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498
```

```
irq  0: 776561217 timer              irq  8:         2 rtc
irq  1:    276048 i8042              irq  9:     24300 VIA8233
irq  2:         0 cascade [4]       irq 11:  38610118 acpi, eth0, uhci_hcd
irq  3:         3                    irq 12:   3435071 i8042
irq  4:         3                    irq 14:   2236471 ide0
irq  6:         2                    irq 15:       251 ide1
```

Pour afficher toutes les informations, utilisez le paramètre `-a`. Le paramètre `-nN` met à jour les informations toutes les *N* secondes. Dans ce cas, arrêtez le programme en appuyant sur la touche Q.

Par défaut, les valeurs cumulées sont affichées. Le paramètre `-d` génère des valeurs différentielles. La commande `procinfo -dn5` affiche les valeurs qui ont changé au cours des cinq dernières secondes :

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer               irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard            irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]         irq 12:       132 PS/2 Mouse
irq  6:         0                     irq 14:         0 ide0
irq  8:         0 rtc                 irq 15:         0 ide1
irq  9:         0 acpi
```

25.16 Ressources PCI : lspci

La commande `lspci` répertorie les ressources PCI :

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
 VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
 VT8366/A/7 [Apollo KT266/A/333 AGP]
```

```
00:0b.0 Ethernet controller: Digital Equipment Corporation \
 DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
 PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
 VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
 MGA G550 AGP (rev 01)
```

Pour obtenir une liste encore plus détaillée, utilisez l'option `-v` :

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
  (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
 Memory at d8000000 (32-bit, prefetchable) [size=32M]
 Memory at da000000 (32-bit, non-prefetchable) [size=16K]
 Memory at db000000 (32-bit, non-prefetchable) [size=8M]
 Expansion ROM at <unassigned> [disabled] [size=128K]
 Capabilities: <available only to root>
```

Les informations sur la résolution des noms de périphérique sont tirées du fichier `/usr/share/pci.ids`. Les ID PCI qui ne figurent pas dans ce fichier sont signalés comme périphériques inconnus (« Unknown device »).

Le paramètre `-vv` génère toutes les informations que le programme a pu obtenir par requête. Pour afficher les valeurs numériques pures, vous devez utiliser le paramètre `-n`.

25.17 Appels système d'une exécution de programme : strace

L'utilitaire `strace` vous permet de tracer tous les appels système d'un processus en cours d'exécution. Entrez la commande normalement, puis ajoutez `strace` au début de la ligne :

```
$ strace -e open ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Par exemple, pour tracer toutes les tentatives d'ouverture d'un fichier particulier, utilisez la commande suivante :

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)       = 3
open("/lib/tls/librt.so.1", O_RDONLY)    = 3
open("/lib/libacl.so.1", O_RDONLY)       = 3
open("/lib/libselinux.so.1", O_RDONLY)   = 3
open("/lib/tls/libc.so.6", O_RDONLY)     = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)      = 3
```

```
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Pour tracer tous les processus enfants, utilisez le paramètre `-f`. Vous pouvez contrôler très précisément le comportement et le format de sortie de la commande strace. Pour plus d'informations, consultez la page `man strace`.

25.18 Appels de bibliothèque d'une exécution de programme : ltrace

La commande `ltrace` vous permet de tracer les appels bibliothèque d'un processus. Cette commande s'utilise comme la commande `strace`. Le paramètre `-c` affiche le nombre et la durée des appels de bibliothèque effectués :

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

25.19 Spécification de la bibliothèque requise : ldd

Vous pouvez utiliser la commande `ldd` pour connaître les bibliothèques qui chargent l'exécutable dynamique spécifié comme argument :

```
$ ldd /bin/ls
```

```
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Les fichiers binaires statiques n'ont besoin d'aucune bibliothèque dynamique :

```
$ ldd /bin/sash
        not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

25.20 Informations supplémentaires sur les fichiers binaires ELF

Vous pouvez lire le contenu des fichiers binaires avec l'utilitaire `readelf`. Cela fonctionne même avec des fichiers ELF construits pour d'autres architectures matérielles :

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

25.21 Communication entre processus : ipcs

La commande `ipcs` génère la liste des ressources IPC en cours d'utilisation :

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

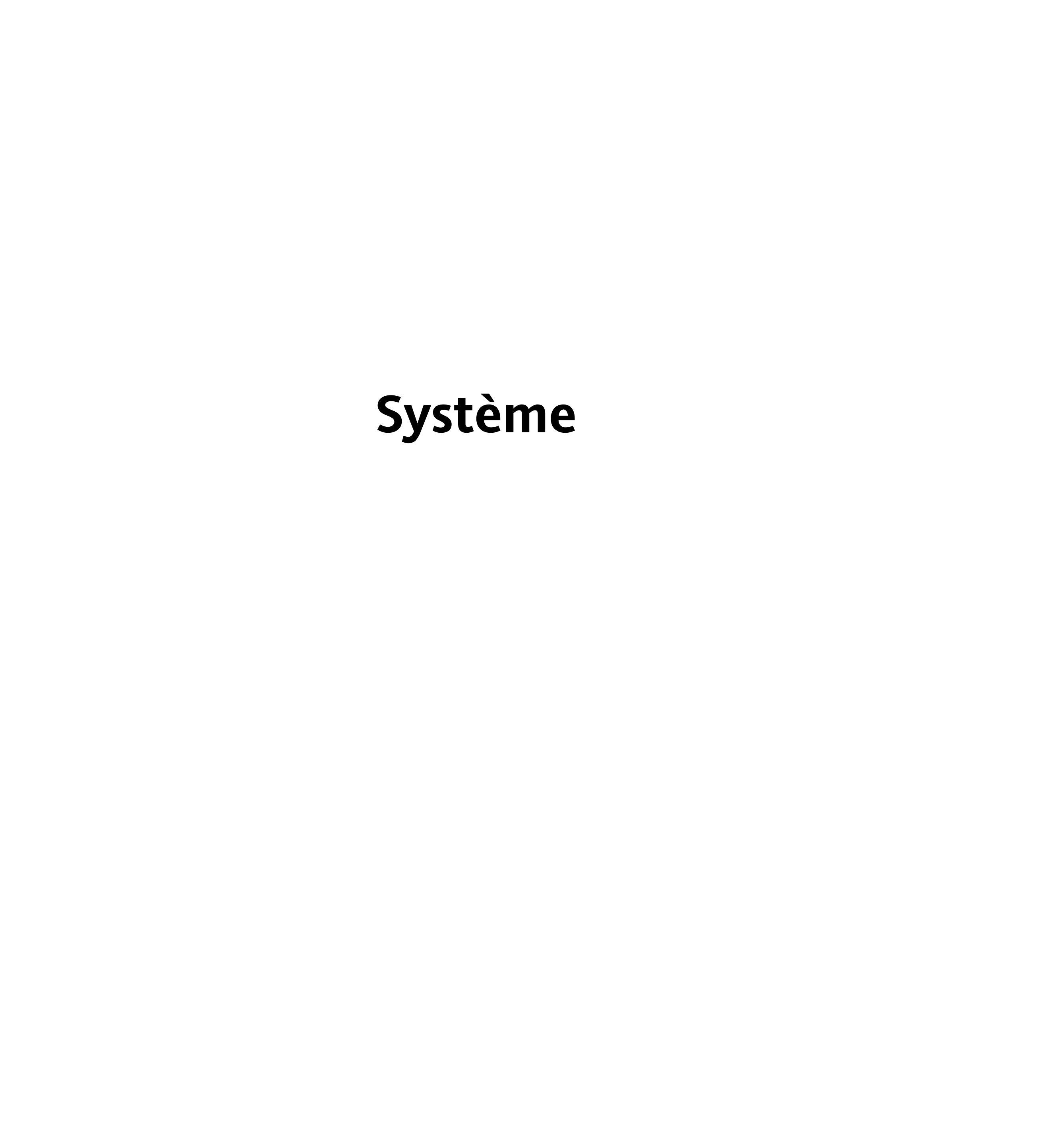
------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

25.22 Calculs de durée avec time

Vous pouvez déterminer le temps d'exécution des commandes avec l'utilitaire `time`. Cet utilitaire offre deux versions : un module intégré au shell et un programme distinct (`/usr/bin/time`).

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```



Système

Applications 32 bits et 64 bits dans un environnement système 64 bits

26

SUSE Linux est disponible pour plusieurs plates-formes 64 bits. Cela ne veut pas forcément dire que toutes les applications fournies avec ont déjà été transférées sur des plates-formes 64 bits. SUSE Linux prend en charge l'utilisation d'applications 32 bits dans un environnement système 64 bits. Ce chapitre vous propose une brève présentation de la mise en œuvre de cette prise en charge sur les plates-formes SUSE Linux 64 bits. Il explique comment les applications 32 bits sont exécutées (prise en charge de l'exécution) et comment vous devez les compiler pour les exécuter aussi bien sur des environnements système 32 bits que 64 bits. De plus, vous obtiendrez des informations sur l'API du kernel, ainsi qu'une explication sur comment les applications 32 bits peuvent être exécutées avec un kernel 64 bits.

SUSE Linux pour les plates-formes 64 bits AMD64 et EM64T a été conçu de sorte à ce qu'il soit possible d'exécuter les applications 32 bits existantes « prêtes à l'emploi » dans des environnements 64 bits. Grâce à cette prise en charge, vous pouvez continuer à utiliser vos applications 32 bits habituelles sans attendre la mise à disposition d'un port 64 bits correspondant.

26.1 Prise en charge de l'exécution

IMPORTANT: Conflits entre les versions des applications

Si une application est disponible à la fois pour les environnements 32 bits et 64 bits, l'installation en parallèle de ces deux versions entraînera forcément

des problèmes. Dans de tels cas, décidez laquelle de ces deux versions installer et utiliser.

Pour que toutes les applications soient correctement exécutées, elles requièrent chacune toute une gamme de bibliothèques. Malheureusement, les noms des versions 32 bits et 64 bits de ces bibliothèques sont identiques. Vous devez donc les différencier.

La compatibilité avec la version 32 bits est possible en stockant les bibliothèques au même emplacement dans votre système que dans l'environnement 32 bits. La version 32 bits de `libc.so.6` se situe dans `/lib/libc.so.6` dans les deux environnements 32 bits et 64 bits.

Toutes les bibliothèques et tous les fichiers d'objets 64 bits sont situés dans des répertoires `lib64`. Les fichiers d'objets 64 bits que vous vous attendriez à trouver normalement dans les répertoires `/lib`, `/usr/lib` et `/usr/X11R6/lib` sont maintenant dans les répertoires `/lib64`, `/usr/lib64` et `/usr/X11R6/lib64`. Cela signifie qu'il y a de l'espace disponible pour les bibliothèques 32 bits dans `/lib`, `/usr/lib` et `/usr/X11R6/lib` : les noms de fichier peuvent donc rester les mêmes dans les deux versions.

Quant aux sous-répertoires des répertoires d'objets dont les données ne dépendent pas de la taille du mot, aucun d'entre eux n'est déplacé. Par exemple, les polices X11 restent à leur emplacement habituel : `/usr/X11R6/lib/X11/fonts`. Ce modèle est conforme aux normes LSB (Linux Standards Base - normes Linux de base) et FHS (File System Hierarchy Standard - norme pour la hiérarchisation du système de fichiers).

26.2 Développement de logiciels

Une chaîne d'outils de développement biarch (à double architecture) permet de générer des objets 32 bits et 64 bits. Par défaut, ce sont des objets 64 bits qui sont compilés. Il est possible de générer des objets 32 bits en utilisant des drapeaux spéciaux. Dans GCC (GNU Compiler Collection - collection de compilateurs GNU), ce drapeau spécial est `-m32`.

Tous les fichiers d'en-tête doivent être rédigés dans un format indépendant de l'architecture. Les bibliothèques 32 bits et 64 bits doivent avoir une API (Application Programming Interface - interface de programmation d'applications) qui correspond aux fichiers d'en-tête installés. L'environnement SUSE normal a été conçu en respectant ce principe.

Dans le cas de bibliothèques mises à jour manuellement, résolvez vous-même ces problèmes.

26.3 Compilation de logiciels sur des plates-formes biarch (à double architecture)

Pour développer des programmes binaires pour la seconde architecture d'une architecture double (biarch), vous devez installer en plus les bibliothèques correspondant à cette seconde architecture. Ces paquetages sont appelés `rpmname-32bit`. Vous avez également besoin des en-têtes et des bibliothèques respectives des paquetages `rpmname-devel`, ainsi que des bibliothèques de développement de la seconde architecture issues de `rpmname-devel-32bit`.

La plupart des programmes « Open Source » utilisent une configuration des programmes basée sur la commande `autoconf`. Pour utiliser `autoconf` pour configurer un programme pour la seconde architecture, écrasez les paramètres normaux du compilateur et de l'éditeur de liens de la commande `autoconf` en exécutant le script `configure` avec d'autres variables d'environnement.

L'exemple suivant fait référence à un système AMD64 ou EM64T avec x86 comme seconde architecture :

1. Paramétrez `autoconf` pour utiliser le compilateur 32 bits :

   ```
   CC="gcc -m32"
   ```

2. Donnez l'instruction à l'éditeur de liens de traiter des objets 32 bits :

   ```
   LD="ld -m elf64_i386"
   ```

3. Paramétrez l'assembleur pour générer des objets 32 bits :

   ```
   AS="gcc -c -m32"
   ```

4. Indiquez que les bibliothèques pour `libtool` et autres sont issues du répertoire `/usr/lib` :

```
LDFLAGS="-L/usr/lib"
```

5. Indiquez que les bibliothèques sont stockées dans le sous-répertoire `lib` :

   ```
   --libdir=/usr/lib
   ```

6. Indiquez que ce sont les bibliothèques X 32 bits qui sont utilisées :

   ```
   --x-libraries=/usr/X11R6/lib/
   ```

Ces variables ne sont pas toutes requises pour chaque programme. Adaptez-en l'utilisation selon le programme.

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
  .configure       \
    --prefix=/usr  \
    --libdir=/usr/lib64
make
make install
```

26.4 Spécifications du kernel

Les kernels 64 bits pour AMD64 et EM64T offrent tous les deux une ABI (Application Binary Interface - interface de définition de la communication entre les applications et le système) de kernel 64 bits et 32 bits. Cette dernière est identique à l'ABI du kernel 32 bits correspondant. Ainsi, l'application 32 bits peut communiquer avec le kernel 64 bits de la même manière qu'avec le kernel 32 bits.

L'émulation 32 bits des appels système d'un kernel 64 bits ne prend pas en charge plusieurs des API utilisées par les programmes système. Cela dépend de la plate-forme. Aussi, vous devez compiler en 64 bits un petit nombre d'applications, telles que `lspci` ou les programmes d'administration LVM, pour qu'elles fonctionnent correctement.

Un kernel 64 bits ne peut charger que des modules de kernel 64 bits qui ont été spécialement compilés pour ce kernel. Il n'est pas possible d'utiliser des modules de kernel 32 bits.

ASTUCE

Certaines applications requièrent des modules chargeables via le kernel. Si vous avez l'intention d'utiliser ce type d'application 32 bits dans un environnement système 64 bits, contactez le fabricant de cette application ainsi que SUSE pour vérifier que la version 64 bits du module chargeable via le kernel et la version compilée 32 bits de l'API du kernel sont disponibles pour ce module.

27 Utilisation du shell

Les interfaces utilisateur graphiques sont de plus en plus importantes pour Linux, mais l'utilisation de la souris n'est pas toujours le meilleur moyen d'effectuer des tâches journalières. La ligne de commande offre une flexibilité et une efficacité élevées. Les applications à base de texte sont particulièrement importantes pour contrôler les ordinateurs sur des liaisons réseau lentes ou si vous souhaitez exécuter des tâches en tant qu'utilisateur `root` sur la ligne de commande d'un terminal X. Le shell Bash est l'interpréteur de ligne de commande par défaut dans SUSE Linux.

Linux est un système multi-utilisateurs. L'accès aux fichiers est contrôlé par les autorisations des utilisateurs. Que vous utilisiez la ligne de commande ou une interface utilisateur graphique, il est utile de comprendre le concept d'autorisation. Lorsque vous utilisez la ligne de commande, un certain nombre de commandes sont importantes. L'éditeur de texte vi est souvent utilisé pour configurer un système à partir de la ligne de commande. Il est également apprécié par un grand nombre d'administrateurs système et de développeurs.

27.1 Utilisation de Bash sur la ligne de commande

La barre des tâches KDE comprend une icône représentant un moniteur avec un coquillage. Lorsque vous cliquez sur cette icône, une fenêtre de terminal s'ouvre dans laquelle vous pouvez entrer des commandes. Konsole, le programme de terminal, exécute normalement Bash (Bourne again shell), un programme développé dans le cadre du projet GNU . Sur le bureau GNOME, cliquez sur une icône de moniteur d'or-

dinateur dans le tableau de bord supérieur pour démarrer un terminal qui exécute normalement Bash.

Une fois que vous avez ouvert le shell, lisez l'invite de la première ligne. L'invite comprend généralement le nom de l'utilisateur, le nom de l'hôte et le chemin actuel, mais peut être personnalisée. Lorsque le curseur se trouve après cette invite, vous pouvez directement envoyer des commandes vers votre système informatique.

27.1.1 Saisie des commandes

Une commande se compose de plusieurs éléments. Le premier élément est toujours la commande réelle, suivie des paramètres ou des options. Les commandes sont exécutées lorsque vous appuyez sur Entrée. Avant de le faire, vous pouvez modifier facilement la ligne de commande, ajouter des options ou corriger des erreurs de frappe. L'une des commandes les plus fréquemment utilisées est `ls`, qu'il est possible d'utiliser avec ou sans arguments. L'entrée de la simple commande `ls` affiche le contenu du répertoire actuel.

Les options sont précédées d'un tiret. Par exemple, la commande `ls -l` affiche le contenu du même répertoire en détail (format de liste long). À côté de chaque nom de fichier figurent la date de création du fichier, la taille du fichier en octets et de plus amples détails qui seront présentés ultérieurement. `--help` est une option importante qui existe pour de nombreuses commandes. En entrant `ls --help` , vous affichez toutes les options de la commande`ls`.

Il est important que la « mise entre guillemets » soit correcte. Si un nom de fichier contient un espace, ignorez l'espace en utilisant une barre oblique inverse (\) ou entourez le nom du fichier de guillemets simples ou doubles. Sinon, Bash interprète un nom tel que `Mes documents` comme les noms de deux fichiers ou de deux répertoires. La différence entre des guillemets simples ou doubles est la suivante : l'expansion de variable se produit avec les guillemets doubles. Les guillemets simples assurent que le shell voit littéralement la chaîne entre guillemets.

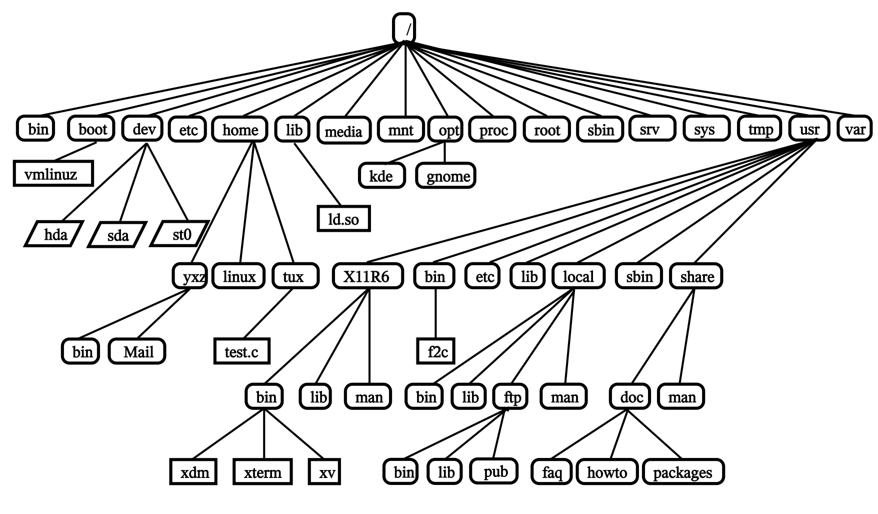
27.1.2 Fichiers et répertoires

Pour utiliser efficacement le shell, il est vraiment utile d'avoir des connaissances sur les structures des fichiers et répertoires d'un système Linux. Vous pouvez envisager les répertoires comme des dossiers électroniques dans lesquels sont stockés les fichiers,

les programmes et les sous-répertoires. Le dossier en haut de la hiérarchie est le répertoire racine, désigné par `/`. C'est l'emplacement à partir duquel vous pouvez accéder à l'ensemble des autres répertoires.

Le répertoire `/home` contient les répertoires dans lesquels chaque utilisateur peut stocker ses fichiers personnels. La Figure 27.1, « Extrait d'une arborescence de répertoires standard » (p. 419) affiche l'arborescence standard de Linux, avec les répertoires maison des exemples d'utilisateurs `xyz`, `linux` et `tux`. L'arborescence d'un système Linux possède une structure fonctionnelle qui suit le *Filesystem Hierarchy Standard* (FHS). La liste suivante offre une brève description des répertoires standard de Linux.

***Figure 27.1** Extrait d'une arborescence de répertoires standard*



/

Répertoire racine, point de départ de l'arborescence

`/home`

Répertoires privés des utilisateurs

`/dev`

Périphériques qui représentent les composants matériels

`/etc`

Fichiers importants pour la configuration du système

/etc/init.d
Commandes de démarrage

/usr/bin
Programmes généralement accessibles

/bin
Programmes requis au début du processus de démarrage

/usr/sbin
Programmes réservés à l'administrateur système

/sbin
Programmes réservés à l'administrateur système et nécessaires au démarrage

/usr/include
Fichiers d'en-tête pour le compilateur C

/usr/include/g++
Fichiers d'en-tête pour le compilateur C++

/usr/share/doc
Divers fichiers de documentation

/usr/share/man
Pages de manuel du système

/usr/src
Code source du système logiciel

/usr/src/linux
Code source du kernel

/tmp, **/var/tmp**
Fichiers temporaires

/usr
Tous les programmes d'applications

/var
Fichiers de configuration (par exemple, ceux liés à `/usr`)

`/var/log`
Fichiers journaux du système

`/var/adm`
Données d'administration du système

`/lib`
Librairies partagées (pour les programmes à lien dynamique)

`/proc`
Système de fichiers de processus

`/sys`
Système de fichiers du système dans lequel toutes les informations de périphérique du kernel sont recueillies

`/usr/local`
Extensions locales indépendantes de la distribution

`/opt`
Logiciel optionnel, paquetages de programmes supplémentaires (tels que KDE, GNOME, Netscape)

27.1.3 Fonctions de Bash

Le shell comporte deux fonctions importantes qui peuvent faciliter largement votre travail :

Historique
Pour répéter une commande entrée précédemment, appuyez sur ↑ jusqu'à ce que la commande précédente apparaisse à l'invite. Pour parcourir la liste des commandes entrées précédemment, appuyez sur ↓. Pour modifier la ligne de commande, il vous suffit de déplacer le curseur jusqu'à la position souhaitée en utilisant les touches fléchées et de commencer à taper. Pour effectuer une recherche dans l'historique, appuyez sur Ctrl + R.

Achèvement
Complète le nom d'un fichier après la saisie de ses premières lettres jusqu'à ce qu'il puisse être identifié de manière univoque. Pour ce faire, tapez les premières lettres,

puis appuyez sur Tab. S'il existe plusieurs noms de fichiers débutant par les mêmes lettres, appuyez deux fois sur Tab pour en obtenir la liste.

Premier exemple : Gestion des fichiers

Maintenant que vous savez à quoi ressemble une commande, quels sont les répertoires qui existent dans SUSE Linux, et comment accélérer les choses à l'aide de Bash, vous pouvez mettre ces connaissances en pratique au moyen d'un petit exercice.

1. Ouvrez une console à partir du bureau de KDE ou de GNOME en cliquant sur l'icône en forme de coquillage.

2. Entrez la commande `ls` pour afficher le contenu de votre répertoire maison.

3. Utilisez la commande `mkdir` (qui signifie *make directory*) pour créer un nouveau sous-répertoire appelé `test` en entrant `mkdir test`.

4. Lancez maintenant un éditeur en appuyant sur Alt + F2 et en entrant `kate` Kate dans KDE `gedit` pour Gedit dans GNOME. Tapez quelques lettres dans l'éditeur, puis enregistrez le fichier sous `Testfile` dans votre dossier personnel. Linux fait la différence entre les majuscules et les minuscules. Pour cet exemple, utilisez la majuscule T.

5. Affichez de nouveau le contenu de votre répertoire maison. Au lieu de taper de nouveau `ls`, il vous suffit d'appuyer deux fois sur ↑ et la commande `ls` doit réapparaître à l'invite. Pour exécuter la commande, appuyez sur Entrée. Le nouveau répertoire `test` doit apparaître en lettres bleues et `Testfile` en noir. C'est ainsi qu'il est possible de différencier les répertoires dans une console.

6. Déplacez `Testfile` dans le sous-répertoire `test` au moyen de la commande `mv`. Pour aller plus vite, utilisez la fonction d'expansion : il vous suffit d'entrer `mv T` et d'appuyer sur Tab. Tant qu'il n'existe pas d'autre fichier débutant par cette lettre dans le répertoire, le shell développe le nom du fichier et ajoute la chaîne *estfile*. Sinon, ajoutez vous-même une lettre ou deux et appuyez à chaque fois sur Tab pour voir si le shell peut développer le nom. Enfin, tapez un espace puis `test` après le nom du fichier développé et appuyez sur Entrée pour exécuter la commande.

7. À ce stade, `Testfile` ne doit plus se trouver dans le répertoire. Pour vérifier, entrez de nouveau `ls`.

8. Pour voir si le fichier a été déplacé avec succès, accédez au répertoire `test` à l'aide de la commande `cd test`. À présent, entrez de nouveau `ls`. Vous devez voir apparaître `Testfile` dans la liste. Vous pouvez revenir à votre répertoire maison à tout moment en tapant seulement `cd`.

9. Pour effectuer une copie d'un fichier, utilisez la commande `cp`. Par exemple, entrez `cp Testfile Testbackup` pour copier `Testfile` dans `Testbackup`. De nouveau, vous pouvez utiliser la commande `ls` pour voir si les deux fichiers se trouvent dans le répertoire.

27.1.4 Spécification des chemins

Lorsque vous travaillez avec des fichiers ou des répertoires, il est important de spécifier le chemin correct. Il est toutefois inutile d'entrer le chemin entier (absolu) depuis le répertoire racine jusqu'au fichier respectif. Vous pouvez partir du répertoire actuel. Accédez directement à votre répertoire maison grâce à ~. Cela signifie qu'il existe deux moyens de lister le fichier `Testfile` dans le répertoire `test` : en entrant le chemin relatif avec `ls test` ou en spécifiant le chemin absolu avec `ls ~/test`.

Pour lister le contenu des répertoires maison d'autres utilisateurs, entrez `ls ~username`. Dans l'exemple d'arborescence, l'un des utilisateurs exemples est `tux`. Dans ce cas, `ls ~tux` listerait le contenu du dossier personnel de `tux`.

Le répertoire actuel est marqué par un point (`.`). Le niveau supérieur suivant de l'arborescence est représenté par deux points (`..`). En entrant `ls ..`, vous affichez le contenu du répertoire parent du répertoire actuel. La commande `ls ../..` affiche le contenu du répertoire deux niveaux plus haut dans la hiérarchie.

Second exemple : utilisation des chemins

Voici un autre exemple illustrant la manière dont vous pouvez vous déplacer dans les répertoires de votre système SUSE Linux.

1. Accédez à votre répertoire maison à l'aide de la commande `cd`. Créez ensuite à cet endroit un répertoire appelé `test2` en tapant `mkdir test2`.

2. Accédez au nouveau répertoire en tapant `cd test2` et créez à cet endroit un sous-répertoire appelé `subdirectory`. Pour y accéder, utilisez la fonction

d'expansion : entrez `cd su`, puis appuyez sur Tab. Le shell développe le reste du nom du répertoire.

3. Essayez à présent de déplacer le fichier créé précédemment `Testbackup` dans le répertoire actuel (`subdirectory`) sans modifier de nouveau le répertoire. Pour ce faire, spécifiez le chemin relatif à ce fichier : `mv ../../test/Testbackup .` (notez le point à la fin). Le point figurant à la fin de cette commande est nécessaire pour indiquer au shell que le répertoire actuel est la destination vers laquelle déplacer le fichier. `../../`, dans cet exemple, se réfère à votre dossier personnel.

27.1.5 Caractères jokers

Le shell propose encore un autre avantage, à savoir les caractères jokers pour l'expansion du nom de chemin. Il en existe trois types différents dans Bash :

?
: Correspond précisément à un caractère arbitraire

*****
: Correspond à un nombre quelconque de caractères

[set]
: Correspond à l'un des caractères du groupe spécifié à l'intérieur des crochets, qui est représenté ici par la chaîne *set*. Dans *set* vous pouvez également spécifier des classes de caractères utilisant la syntaxe *[:class:]*, où une classe est un `alnum`, `alpha`, `ascii`, etc.

  L'utilisation de `!` ou de `^` au début du groupe (*[!set]*) correspond à un caractère autre que celui identifié par *set*.

En supposant que votre répertoire `test` contienne les fichiers `Testfile`, `Testfile1`, `Testfile2` et `datafile`, la commande `ls Testfile?` liste les fichiers `Testfile1` et `Testfile2`. Avec `ls Test*`, la liste inclut également `Testfile`. `ls *fil*` affiche tous les fichiers exemples. Enfin, vous pouvez utiliser le caractère joker `set` pour accéder à tous les fichiers exemples dont le dernier caractère est un nombre : `ls Testfile[1-9]` ou, en utilisant des classes, `ls Testfile[[:digit:]]`.

Sur les quatre types de caractères jokers, le plus inclusif est l'astérisque. Il peut servir à copier tous les fichiers contenus dans un répertoire vers un autre ou supprimer tous les fichiers à l'aide d'une commande. La commande `rm *fil*`, par exemple, supprimerait tous les fichiers du répertoire actuel dont le nom comprend la chaîne *fil*.

27.1.6 Less et More

Linux comprend deux petits programmes permettant d'afficher des fichiers texte directement dans le shell. Au lieu de lancer un éditeur pour lire un fichier tel que `Lisezmoi.txt`, il vous suffit d'entrer `less Lisezmoi.txt` pour afficher le texte dans la fenêtre de console. Utilisez la barre d'[espace] pour faire défiler une page vers le bas. Utilisez les touches [Page suivante] et [Page précédente] pour avancer ou reculer dans le texte. Pour quitter less, appuyez sur [Q].

Au lieu de less, vous pouvez également utiliser l'ancien programme more. Il est toutefois moins pratique car il ne permet pas de faire défiler en arrière.

Le programme less tire son nom du précepte selon lequel *moins vaut plus* et peut servir également à afficher la sortie des commandes de façon appropriée. Pour comprendre son fonctionnement, consultez Section 27.1.7, « Tuyaux et redirection » (p. 425).

27.1.7 Tuyaux et redirection

En principe, la sortie standard du shell est votre écran ou la fenêtre de console, et l'entrée standard le clavier. Pour transférer la sortie d'une commande vers une application telle que less, vous pouvez utiliser un *tuyau*.

Pour afficher les fichiers dans le répertoire `test`, entrez la commande `ls test | less`. Le contenu du répertoire `test` s'affiche ensuite avec less. Cela est utile uniquement si la sortie normale avec `ls` est trop longue. Par exemple, si vous affichez le contenu du répertoire `dev` avec la commande `ls /dev`, vous ne voyez qu'une petite partie de la fenêtre. Pour voir la liste entière, tapez `ls /dev | less`.

Il est possible également d'enregistrer la sortie des commandes dans un fichier. Par exemple, `echo "test one" > Content` génère un nouveau fichier nommé `Content` qui contient les mots `test one`. Pour afficher le fichier, tapez `less Content`.

Vous pouvez également utiliser un fichier comme entrée d'une commande. Par exemple, `tr` remplace les caractères de l'entrée standard qui redirigeait à partir du fichier `Content` et écrit le résultat dans la sortie standard : remplacer `t` par `x` en appelant `tr t x < Content`. La sortie de la commande `tr` est envoyée à l'écran.

Si vous avez besoin d'un nouveau fichier contenant la sortie, il suffit de transmettre la sortie de `tr` dans un fichier. En guise de test, changez pour `test` et saisissez la commande `tr t x < ../Content > new`. Enfin, affichez `new` avec `less new`.

Tout comme la sortie standard, le message d'erreur standard est envoyé vers la console. Cependant, pour rediriger le message d'erreur standard vers un fichier appelé `errors`, vous devez ajouter `2> errors` à la commande correspondante. La sortie et le message d'erreur standard sont tous deux enregistrés dans un fichier appelé `alloutput` si vous ajoutez `>& alloutput`. Enfin, pour ajouter la sortie d'une commande à un fichier déjà existant, la commande doit être suivie par `>>` au lieu de `>`.

27.1.8 Archives et compression des données

Maintenant que vous avez créé plusieurs fichiers et répertoires, vous pouvez aborder le thème des archives et de la compression de données. Supposez que vous voulez avoir le répertoire `test` complet compacté dans un fichier que vous pouvez enregistrer sur une clé USB comme copie de sauvegarde ou envoyer par courrier électronique. Pour ce faire, utilisez la commande `tar` (pour *tape archiver*). A l'aide de la commande `tar --help`, affichez ensuite toutes les options de la commande `tar`. Les options les plus importantes sont expliquées ici :

-c
: (pour create) Crée une nouvelle archive.

-t
: (pour table) Affiche le contenu d'une archive.

-x
: (pour extract) Décompacte l'archive.

-v
: (pour verbose) Affiche tous les fichiers à l'écran pendant la création de l'archive.

-f

(pour file) Choisit un nom de fichier pour le fichier de l'archive. Lorsque vous créez une archive, cette option doit toujours être indiquée en dernière.

Pour compacter le répertoire `test` avec tous ses fichiers et sous-répertoires dans une archive appelée `testarchive.tar`, utilisez les options `-c` et `-f`. Aux fins de test, ajoutez également `-v` pour suivre la progression de l'archivage, même si cette option n'est pas obligatoire. Après avoir utilisé `cd` pour accéder à votre répertoire maison dans lequel se trouve le répertoire `test`, entrez `tar -cvf testarchive.tar test`. Après cela, affichez le contenu du fichier d'archive à l'aide de la commande `tar -tf testarchive.tar`. Le répertoire `test` et tous ses fichiers et répertoires restent inchangés sur votre disque dur. Pour décompacter l'archive, il vous suffit d'entrer `tar -xvf testarchive.tar`, mais ne le faites pas encore.

Pour la compression des fichiers, le choix évident est `gzip` ou, pour un rapport de compression encore meilleur, `bzip2`. Il suffit de saisir `gzip testarchive.tar` (ou `bzip2 testarchive.tar`, mais c'est `gzip` qui est utilisé dans cet exemple). Grâce à la commande `ls`, vous voyez à présent que le fichier `testarchive.tar` n'est plus là et que le fichier `testarchive.tar.gz` a été créé à sa place. Ce fichier est beaucoup plus petit et, par conséquent, convient beaucoup mieux au transfert par courrier électronique ou au stockage sur clé USB.

À présent, décompactez ce fichier dans le répertoire `test2` créé précédemment. Pour ce faire, tapez `cp testarchive.tar.gz test2` afin de copier le fichier dans ce répertoire. Accédez au répertoire à l'aide de la commande `cd test2`. Une archive compactée portant l'extension `.tar.gz` peut être dézippée à l'aide de la commande `gunzip`. Entrez `gunzip testarchive.tar.gz`, qui a pour résultat le fichier `testarchive.tar`, lequel doit ensuite être extrait ou *décompacté* à l'aide de la commande `tar -xvf testarchive.tar`. Vous pouvez également dézipper et extraire une archive compactée en une seule opération avec `tar -xvf testarchive.tar.gz` (l'ajout de l'option `-z` n'est plus nécessaire). La commande `ls` permet de constater qu'un nouveau répertoire `test` a été créé avec le même contenu que votre répertoire `test` dans votre répertoire maison.

27.1.9 mtools

`mtools` comprend un ensemble de commandes permettant de travailler avec les systèmes de fichiers MS-DOS. Les commandes incluses dans `mtools` permettent de

désigner la première disquette par `a:`, comme sous MS-DOS, et les commandes sont identiques à celles de MS-DOS, sauf qu'elles sont précédées du préfixe `m` :

`mdir a:`
Affiche le contenu de la disquette sur le lecteur `a:`

`mcopy Testfile a:`
Copie les fichiers `Testfile` sur la disquette

`mdel a:Testfile`
Supprime `Testfile` sur `a:`

`mformat a:`
Formate la disquette dans le format MS-DOS (à l'aide de la commande `fdformat`)

`mcd a:`
Fait de `a:` votre répertoire actuel

`mmd a:test`
Créé le sous-répertoire `test` sur la disquette

`mrd a:test`
Supprime le sous-répertoire `test` de la disquette

27.1.10 Nettoyage

Après ce cours intensif, vous devriez être habitué aux basiques du shell ou de la ligne de commande Linux. Si vous le souhaitez, vous pouvez nettoyer votre répertoire maison en supprimant les différents fichiers et répertoires test grâce aux commandes `rm` et `rmdir`. Dans Section 27.3, « Commandes Linux importantes » (p. 435), vous trouverez une liste des commandes les plus importantes, ainsi qu'une brève description de leurs fonctions.

27.2 Utilisateurs et autorisations d'accès

Depuis sa création au début des années 1990, Linux a été conçu comme un système multi-utilisateurs. Un nombre quelconque d'utilisateurs peut travailler dessus en même temps. Les utilisateurs doivent se loguer au système avant de démarrer une session sur leur poste de travail. Chaque utilisateur possède un nom d'utilisateur et le mot de passe correspondant. Grâce à cette différenciation des utilisateurs, il est garanti que les utilisateurs non autorisés ne pourront pas consulter des fichiers pour lesquels ils ne possèdent pas d'autorisation. Les modifications plus importantes du système, telles que l'installation de nouveaux programmes, sont généralement impossibles ou restreintes pour les utilisateurs normaux. Seul l'utilisateur, ou le *superutilisateur*, possède la capacité non restreinte d'apporter des modifications au système et dispose d'un accès illimité à l'ensemble des fichiers. Quiconque utilise ce concept de façon judicieuse, en se loguant avec un accès `root` complet uniquement lorsque cela est nécessaire, peut réduire le risque de perte non intentionnelle de données. Étant donné qu'en règle générale, seul l'utilisateur root peut supprimer des fichiers ou des systèmes ou formater les disques durs, il est possible de réduire considérablement le risque d'un *effet cheval de Troie* ou d'une entrée accidentelle de commandes destructrices.

27.2.1 Autorisations du système de fichiers

Fondamentalement, chaque fichier d'un système de fichiers Linux appartient à un utilisateur et à un groupe. Chacun de ces groupes propriétaires et tous les autres sont autorisés à écrire, lire ou exécuter ces fichiers.

Dans ce cas, un groupe peut être défini comme un ensemble d'utilisateurs connectés ayant certains droits collectifs. Par exemple, appelez un groupe travaillant sur un certain projet `project3`. Chaque utilisateur d'un système Linux est membre d'au moins un groupe propriétaire, en principe celui des `users`. Un système peut comprendre autant de groupes que nécessaire, mais seul un `superutilisateur` peut ajouter des groupes. La commande `groups` permet à chaque utilisateur de savoir à quel groupe il appartient.

Accès aux fichiers

L'organisation des autorisations du système de fichiers diffère pour les fichiers et les répertoires. Les informations sur les autorisations de fichier peuvent être affichées

à l'aide de la commande `ls -l`. La sortie peut se présenter comme dans l'Exemple 27.1, « Exemple de sortie affichant les autorisations de fichier » (p. 430).

***Exemple 27.1** Exemple de sortie affichant les autorisations de fichier*

```
-rw-r----- 1 tux project3 14197 Jun 21  15:03 Roadmap
```

Comme le montre la troisième colonne, ce fichier appartient à l'utilisateur `tux`. Il est assigné au groupe `project3`. Pour connaître les autorisations d'utilisateur du fichier `Roadmap`, il convient d'examiner la première colonne de plus près.

-	rw-	r--	---
Type	Autorisations d'utilisateur	Autorisations de groupe	Autorisations pour les autres utilisateurs

Cette colonne se compose d'un caractère d'en-tête suivi par neuf caractères groupés par trois par trois. La première des dix lettres représente le type de composant du système de fichiers. Le tiret (`-`) indique qu'il s'agit d'un fichier. Un répertoire (`d`), un lien (`l`), un périphérique de bloc (`b`), ou un périphérique de caractères peuvent également être indiqués.

Les trois blocs suivants sont fondés un modèle standard. Les trois premiers caractères indiquent si le fichier est lisible(`r`) ou non (`-`). Un `w` dans la partie intermédiaire symbolise le fait que l'objet correspondant peut être modifié et un tiret (`-`) signifie qu'il est impossible d'écrire dans le fichier. Un `x` en troisième position signale que l'objet peut être exécuté. Comme le fichier de cet exemple est un fichier texte et non un fichier exécutable, l'accès exécutable n'est pas requis pour ce fichier.

Dans cet exemple, en tant que propriétaire du fichier `Roadmap`, `tux` possède les droits de lecture (`r`) et d'écriture (`w`) sur ce fichier, mais ne peut l'exécuter (`x`). Les membres du groupe `project3` peuvent lire le fichier, mais ne peuvent le modifier ou l'exécuter. Les autres utilisateurs n'ont pas accès à ce fichier. Il est possible d'assigner d'autres autorisations au moyen des ACL (listes de contrôle d'accès). Pour plus d'informations, consultez la Section 27.2.6, « Listes de contrôle d'accès » (p. 434).

Autorisations de répertoire

Les autorisations d'accès pour les répertoires ont le type `d`. Pour les répertoires, les autorisations individuelles ont une signification légèrement différente.

Exemple 27.2 *Exemple de sortie affichant les autorisations de répertoire*

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15  ProjectData
```

Dans l'Exemple 27.2, « Exemple de sortie affichant les autorisations de répertoire » (p. 431), le propriétaire (`tux`) et le groupe propriétaire (`project3`) du répertoire `ProjectData` sont faciles à identifier. Contrairement aux autorisations d'accès aux fichiers de Accès aux fichiers (p. 429), l'autorisation de lecture définie (`r`) signifie qu'il est possible d'afficher le contenu du répertoire. Le droit d'écriture (`w`) implique qu'il est possible de créer de nouveaux fichiers. Le droit d'exécution (x) implique que l'utilisateur peut accéder à ce répertoire. Dans l'exemple précédent, l'utilisateur `tux` ainsi que les membres du groupe `project3` peuvent accéder au répertoire `ProjectData` (`x`), en afficher le contenu (`r`), et lui ajouter ou en supprimer des fichiers (`w`). Les autres utilisateurs ont un accès restreint. Ils peuvent entrer dans le répertoire (`x`) et le parcourir (`r`), mais ne peuvent pas y insérer de nouveaux fichiers (`w`).

27.2.2 Modification des autorisations de fichier

Modification des autorisations d'accès

Les autorisations d'accès d'un fichier ou d'un répertoire peuvent être modifiées par le propriétaire et, bien sûr, par l'utilisateur `root` à l'aide de la commande `chmod`, suivie des paramètres modifiant les autorisations et un ou plusieurs noms de fichiers. Les paramètres constituent des catégories différentes :

1. les utilisateurs concernés

- `u` (*user*) - propriétaire du fichier
- `g` (*group*) - groupe qui détient le fichier
- `o` (*others*) - utilisateurs supplémentaires (si aucun paramètre n'est indiqué, les modifications s'appliquent à toutes les catégories)

2. un caractère de suppression (−), de définition (=) ou d'insertion (+)

3. les abréviations

- `r` - *lire*
- `w` - *écrire*
- `x` - *exécuter*

4. nom de fichier ou noms de fichier séparés par des espaces

Par exemple, si l'utilisateur `tux` de l'Exemple 27.2, « Exemple de sortie affichant les autorisations de répertoire » (p. 431) souhaite accorder le droit d'écriture (`w`) à d'autres utilisateurs sur le répertoire `ProjectData`, il peut le faire à l'aide de la commande `chmod o+w ProjectData`.

En revanche, s'il souhaite supprimer toutes les autorisations d'utilisateurs excepté la sienne, il peut le faire en entrant la commande `chmod go-w ProjectData`. Pour interdire à tous les utilisateurs d'ajouter un nouveau fichier au dossier `ProjectData`, entrez `chmod -w ProjectData`. À présent, même le propriétaire ne peut écrire dans le fichier sans rétablir les droits d'écriture au préalable.

Modifications des autorisations de propriété

Les autres commandes importantes qui permettent de contrôler la propriété et les autorisations des composants du système de fichiers sont `chown` (pour « change owner ») et `chgrp` (pour « change group »). La commande `chown` peut servir à transférer la propriété d'un fichier vers un autre utilisateur. Toutefois, seul un utilisateur `root` est autorisé à effectuer cette modification.

Supposons que le fichier `Roadmap` de l'Exemple 27.2, « Exemple de sortie affichant les autorisations de répertoire » (p. 431) ne doive plus appartenir à `tux`, mais à l'utilisateur `geeko`. L'utilisateur `root` doit alors entrer `chown geeko Roadmap`.

`chgrp` modifie la propriété de groupe du fichier. Toutefois, le propriétaire du fichier doit faire partie du nouveau groupe. De cette manière, l'utilisateur `tux` de l'Exemple 27.1, « Exemple de sortie affichant les autorisations de fichier » (p. 430) peut basculer le groupe propriétaire du fichier `ProjectData` vers `project4` à

l'aide de la commande `chgrp project4 ProjectData`, à condition qu'il soit membre de ce nouveau groupe.

27.2.3 Le bit setuid

Dans certaines situations, les autorisations d'accès peuvent être trop restrictives. C'est pourquoi Linux possède des paramètres supplémentaires permettant de modifier provisoirement l'identité actuelle de l'utilisateur et du groupe pour une action spécifique. Par exemple, le programme `passwd` requiert normalement des autorisations de niveau racine pour accéder à `/etc/passwd`. Ce fichier contient des informations importantes (par exemple, les répertoires privés des utilisateurs, ainsi que les ID des utilisateurs et des groupes). Un utilisateur ordinaire n'est donc pas en mesure de changer le fichier `passwd`, car cela serait trop dangereux d'accorder un accès direct à ce fichier à l'ensemble des utilisateurs. Le mécanisme *setuid* offre une solution à ce problème. setuid (pour « set user ID ») est un attribut de fichier spécial qui indique au système d'exécuter certains programmes sous un ID utilisateur spécifique. Imaginons la commande `passwd` :

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Le `s` indique que le bit setuid est défini pour l'autorisation de l'utilisateur. Grâce au bit setuid, tous les utilisateurs qui lancent la commande `passwd` l'exécutent en tant que `root`.

27.2.4 Le bit setgid

Le bit setuid s'applique aux utilisateurs. Toutefois, il existe également une propriété équivalente pour les groupes : le bit *setgid*. Un programme pour lequel cet attribut a été défini est exécuté sous l'ID groupe sous lequel il a été enregistré, quel que soit l'utilisateur qui le lance. Par conséquent, dans un répertoire comprenant le bit setgid, tous les fichiers et sous-répertoires nouveaux sont assignés au groupe auquel appartient le répertoire. Prenez pour exemple le répertoire suivant :

```
drwxrws--- 2 tux archive 48 Nov 19 17:12
   backup
```

Le `s` indique que le bit setuid est défini pour l'autorisation du groupe. Le propriétaire du répertoire et les membres du groupe `archive` peuvent accéder à ce répertoire. Les utilisateurs qui ne sont pas membres de ce groupe sont « assignés » à leur groupe res-

pectif. L'ID de groupe effectif de tous les fichiers écrits sera `archive`. Par exemple, un programme de sauvegarde qui est exécuté avec l'ID de groupe `archive` peut accéder à ce répertoire, même s'il n'est pas doté des privilèges de niveau racine.

27.2.5 Le bit autocollant

Il existe également le *bit autocollant*. Son utilisation est différente selon qu'il appartient à un programme exécutable ou à un répertoire. S'il appartient à un programme, un fichier marqué de cette façon est chargé dans la mémoire RAM pour éviter d'avoir à l'extraire du disque dur à chacune de ces utilisations. Cet attribut est rarement utilisé car les disques durs modernes sont suffisamment rapides. Si ce bit est assigné à un répertoire, il empêche les utilisateurs de supprimer leurs fichiers respectifs. Des exemples typiques sont les répertoires `/tmp` et `/var/tmp` :

```
drwxrwxrwt   2 root  root   1160 2002-11-19 17:15 /tmp
```

27.2.6 Listes de contrôle d'accès

Le concept classique d'autorisation pour les objets du système de fichiers Linux, tels que les fichiers ou les répertoires, peut être développé au moyen des ACL (listes de contrôle d'accès). Elles permettent d'assigner des autorisations à des utilisateurs ou groupes individuels autres que le propriétaire ou le groupe propriétaire d'origine d'un objet du système de fichiers.

Les fichiers ou répertoires qui comportent des autorisations d'accès étendues peuvent être détectés à l'aide d'une simple commande `ls -l` :

```
-rw-r--r--+ 1 tux project3 14197 Jun 21  15:03 Roadmap
```

`Roadmap` est détenu par `tux` qui appartient au groupe `project3`. `tux` possède à la fois les droits d'écriture et de lecture sur ce fichier. Son groupe, comme tous les autres utilisateurs, possèdent des droits de lecture. La seule différence qui distingue ce fichier d'un fichier sans ACL est le + supplémentaire qui apparaît dans la première colonne comportant les bits d'autorisation.

Pour obtenir des détails sur l'ACL, exécutez la commande `getfacl Roadmap` :

```
# file: Roadmap
# owner: tux
# group: project3
user::rw-
```

```
user:jane:rw-        effective: r--
group::r--
group:djungle:rw-    effective: r--
mask::r--
other::---
```

Les trois premières lignes de la sortie ne comportent aucune information qui n'est pas disponible avec la commande `ls -l`. Ces lignes indiquent uniquement le nom du fichier, le propriétaire et le groupe propriétaire. Les lignes 4 à 9 comportent les entrées ACL. Les autorisations d'accès conventionnelles représentent un sous-ensemble des autorisations possibles en utilisant les ACL. Cet exemple d'ACL accorde les droits de lecture et d'écriture au propriétaire du fichier, ainsi qu'à l'utilisateur `jane` (lignes 4 et 5). Le concept conventionnel a été développé pour offrir l'accès à un utilisateur supplémentaire. Le même principe s'applique à la gestion d'un accès de groupe. Le groupe propriétaire possède des droits de lecture (ligne 6) et le groupe `djungle` des droits de lecture et d'écriture. L'entrée de la commande `mask` à la ligne 8 réduit les droits de lecture effectifs de l'utilisateur `jane` et du groupe `djungle`. Les autres utilisateurs et groupes ne bénéficient d'aucun accès au fichier (ligne 9).

Seules des informations très basiques sont fournies ici. Pour plus d'informations sur les ACL, reportez-vous au Chapitre 24, *Listes de contrôle d'accès sous Linux* (p. 377).

27.3 Commandes Linux importantes

Cette section donne un aperçu des commandes les plus importantes de votre système SUSE LINUX. Il existe beaucoup plus de commandes que celles reprises dans ce chapitre. Les paramètres sont listés avec les commandes individuelles et, le cas échéant, un exemple d'application typique est présenté. Pour en savoir plus sur les différentes commandes, utilisez les pages de manuel, accessibles avec `man` suivi du nom de la commande (par exemple, `man ls`).

Pour monter et descendre dans les pages de manuel, utilisez les options Pg préc. et Pg suiv.. Pour passer du début à la fin d'un document, utilisez les options Début et Fin. Quittez ce mode d'affichage en appuyant sur Q. Pour en apprendre davantage sur la commande `man` elle-même, entrez la commande `man man`.

Dans la présentation suivante, les différents éléments de commande sont écrits dans différentes polices. La commande réelle et ses options obligatoires sont toujours imprimées en `option de commande`. Les spécifications ou paramètres qui ne sont pas requis sont placés entre `[crochets]`.

Ajustez les réglages en fonction de vos besoins. Il est inutile d'écrire `ls fichier`, s'il n'existe aucun fichier dénommé `fichier`. Vous pouvez généralement combiner plusieurs paramètres, par exemple en écrivant `ls -la` au lieu de `ls -l -a`.

27.3.1 Commandes des fichiers

La section suivante énumère les commandes les plus importantes en matière de gestion des fichiers. Elle couvre l'ensemble de ces opérations, de l'administration générale des fichiers à la manipulation des ACL de système de fichiers.

Gestion des fichiers

`ls [options] [fichiers]`

Si vous exécutez la commande `ls` sans paramètres supplémentaires, le programme liste le contenu du répertoire actuel sous une forme abrégée.

`-l`
Liste détaillée

`-a`
Affiche les fichiers cachés.

`cp [options] source cible`

Copie la `source` dans la `cible`.

-i
Attend la confirmation, si nécessaire, avant de remplacer la `cible`.

-r
Copie de façon récurrente (y compris les sous-répertoires).

`mv [options] source cible`

Copie la `source` vers la `cible`, puis supprime la `source` d'origine.

-b
Crée une copie de sauvegarde de la `source` avant de la déplacer.

-i

Attend la confirmation, si nécessaire, avant de remplacer le `fichier cible`.

`rm [options] fichiers`

Supprime les fichiers spécifiés du système de fichiers. Les répertoires ne sont pas supprimés par la commande `rm`, à moins que l'option `-r` soit utilisée.

`-r`

Supprime tous les sous-répertoires existants.

`-i`

Attend la confirmation avant la suppression de chaque fichier.

`ln [options] source cible`

Crée un lien interne de la `source` vers la `cible`. En principe, un tel lien pointe directement vers la `source` sur le même système de fichiers. Toutefois, si la commande `ln` est exécutée avec l'option `-s`, elle crée un lien symbolique qui ne pointe que sur le répertoire dans lequel figure la `source`, permettant ainsi de lier les systèmes de fichiers.

-s

Crée un lien symbolique.

`cd [options] [répertoire]`

Modifie le répertoire actuel. `cd` sans paramètres permet d'accéder au répertoire personnel de l'utilisateur.

`mkdir [options] répertoire`

Crée un nouveau répertoire.

`rmdir [options] répertoire`

Supprime le répertoire spécifié s'il est déjà vide.

`chown [options] nomd'utilisateur[:[group]] fichiers`

Transfère la propriété d'un fichier vers l'utilisateur portant le nom spécifié.

-R

Modifie les fichiers et les répertoires dans tous les sous-répertoires.

chgrp [options] nomgroupe fichiers

Transfère la propriété de groupe d'un `fichier` donné vers le groupe portant le nom du groupe spécifié. Le propriétaire du fichier peut modifier uniquement la propriété de groupe s'il fait partie à la fois du groupe actuel et du nouveau groupe.

chmod [options] mode fichiers

Modifie les autorisations d'accès.

Le paramètre `mode` comprend trois parties : `group`, `access` et `access type`. `group` accepte les caractères suivants :

u

utilisateur

g

groupe

o

autres

Pour la commande `access`, accordez les droits avec `+` et refusez-les avec `-`.

La commande `access type` est contrôlée par les options suivantes :

r

lecture

w

écriture

x

execute—exécution des fichiers ou accès au répertoire

s

Setuid bit—l'application ou le programme est lancé comme s'il était lancé par le propriétaire du fichier.

Il est possible également d'utiliser un code numérique. Les quatre chiffres de ce code sont composés de la somme des valeurs 4, 2 et 1 - le résultat décimal d'un masque binaire. Le premier chiffre définit l'ID de l'utilisateur (SUID) (4), l'ID du groupe (2) et les étiquettes autocollantes (1). Le second chiffre définit les autorisations du propriétaire du fichier. Le troisième chiffre définit les autorisations des membres du groupe et le dernier chiffre définit les autorisations de tous les autres utilisateurs. Le droit de lecture est défini par 4, le droit d'écriture par 2, et le droit d'exécution d'un fichier par 1. Le propriétaire d'un fichier reçoit généralement un 6 ou un 7 pour les fichiers exécutables.

`gzip [paramètres] fichiers`

Ce programme compacte le contenu des fichiers au moyen d'algorithmes mathématiques complexes. Les fichiers compactés de cette façon reçoivent l'extension `.gz` et doivent être décompactés avant de pouvoir être utilisés. Pour comprimer plusieurs fichiers ou même des répertoires complets, utilisez la commande `tar`.

-d
Décompacte les fichiers gzip compressés pour qu'ils retrouvent leur taille d'origine et puissent être traités normalement (comme la commande `gunzip`)

`tar options archive fichiers`

`tar` place un ou plusieurs fichiers dans une archive. La compression est facultative. `tar` est une commande tout à fait complexe comprenant plusieurs options. Les options les plus fréquemment utilisées sont :

`-f`
Écrit la sortie dans un fichier et pas à l'écran comme c'est habituellement le cas.

`-c`
Crée une nouvelle archive tar.

`-r`
Ajoute des fichiers à une archive existante.

`-t`
Indique le contenu d'une archive.

-u

Ajoute des fichiers, mais seulement s'ils sont plus récents que les fichiers déjà contenus dans l'archive.

-x

Décompacte les fichiers à partir d'une archive (*extraction*).

-z

Compacte l'archive résultante avec `gzip`.

-j

Compacte l'archive résultante avec `bzip2`.

-v

Liste les fichiers traités.

Les fichiers d'archive créés par `tar` se terminent par `.tar`. Si l'archive tar a été également comprimée à l'aide de la commande `gzip`, l'extension est `.tgz` ou `.tar.gz`. Si elle a été comprimée à l'aide de la commande `bzip2`, l'extension est `.tar.bz2`. Des exemples d'application sont disponibles dans Section 27.1.8, « Archives et compression des données » (p. 426).

`locate modèles`

Cette commande n'est disponible que si vous avez installé le paquetage `findutils-locate`. La commande `locate` permet de localiser le répertoire dans lequel se trouve un fichier spécifié. Si vous le souhaitez, vous pouvez utiliser des jokers pour indiquer les noms de fichiers. Le programme est très rapide, car il utilise une base de données spécialement créée à cet effet (plutôt que de chercher dans tout le système de fichiers). Cela présente toutefois un inconvénient majeur : l'impossibilité de retrouver des fichiers créés après la dernière mise à jour de la base de données. La base de données peut être générée par l'utilisateur `root` à l'aide de la commande `updatedb`.

`updatedb [options]`

Cette commande exécute une mise à jour de la base de données utilisée par la commande `locate`. Pour inclure les fichiers dans tous les répertoires existants, exécutez le programme en tant qu'utilisateur `root`. Il est utile également de le placer en arrière-plan en ajoutant une esperluette (`&`). Vous pouvez ainsi continuer immédiatement à travailler sur la même ligne de commande (`updatedb &`). Cette

commande s'exécute généralement comme une tâche cron quotidienne (voir `cron.daily`).

`find [options]`

La commande `find` permet de rechercher un fichier dans un répertoire donné. Le premier argument spécifie le répertoire dans lequel lancer la recherche. L'option `-name` doit être suivie d'une chaîne de recherche qui peut contenir également des caractères jokers. Contrairement à la commande `locate` qui utilise une base de données, la commande `find` analyse le répertoire actuel.

Commandes permettant d'accéder au contenu des fichiers

`cat [options] fichiers`

La commande `cat` affiche le contenu d'un fichier en imprimant le contenu entier à l'écran sans interruption.

-n
Numérote la sortie dans la marge gauche.

`less [options] fichiers`

Cette commande peut servir à parcourir le contenu du fichier spécifié. Faites défiler la moitié d'une page écran vers le haut ou vers le bas à l'aide des options Pg préc. et Pg suiv. ou une page d'écran complète vers le bas en appuyant sur Espace. Pour atteindre le début ou la fin d'un fichier, utilisez les options Début et Fin. Appuyez sur Q pour quitter le programme.

`grep [options] searchstring fichiers`

La commande grep recherche une chaîne spécifique dans les fichiers spécifiés. Si la chaîne de recherche a été trouvée, la commande affiche la ligne dans laquelle se trouve la `chaînerecherchée`, ainsi que le nom du fichier.

-i
Ignore la casse.

-H

N'affiche que les noms des fichiers respectifs, pas les lignes de texte.

-n

Affiche également les numéros des lignes dans lesquelles une correspondance a été trouvée.

-l

Liste uniquement les fichiers dans lesquels la `chaînerecherchée` ne se trouve pas.

diff [options] fichier 1 fichier 2

La commande `diff` compare le contenu des deux fichiers. La sortie produite par le programme liste toutes les lignes qui ne correspondent pas. Cette commande est fréquemment utilisée par les programmeurs qui ont besoin seulement d'envoyer leurs changements de programme et pas leur code source entier.

-q

Indique uniquement si les deux fichiers diffèrent.

-u

Produit un diff « unifié », qui rend la sortie plus lisible.

Systèmes de fichiers

mount [options] [unité] pointmontage

Cette commande peut servir à monter n'importe quel support de données, comme les disques durs, les lecteurs de CD-ROM et les autres lecteurs, dans un répertoire du système de fichiers Linux.

-r

montage en lecture seule.

-t filesystem

Spécifie le système de fichiers, généralement `ext2` pour les disques durs Linux, `msdos` pour le support MS-DOS, `vfat` pour le système de fichiers Windows et `iso9660` pour les CD.

Pour les disques durs qui ne sont pas définis dans le fichier `/etc/fstab`, il est nécessaire également de spécifier le type de périphérique. Dans ce cas, seul l'utilisateur `root` peut réaliser le montage. Si le système de fichiers doit être également monté par d'autres utilisateurs, entrez l'option `user` dans la ligne appropriée du fichier `/etc/fstab` (séparé par des virgules) et enregistrez cette modification. De plus amples informations sont disponibles dans la page de manuel `mount(1)`.

`umount [options] pointmontage`

Cette commande démonte un lecteur monté du système de fichiers. Pour empêcher la perte de données, exécutez cette commande avant de retirer un support de données amovible de son lecteur. En principe, seul l'utilisateur `root` est autorisé à exécuter les commandes `mount` et `umount`. Pour permettre aux autres utilisateurs d'exécuter ces commandes, modifiez le fichier `/etc/fstab` afin de spécifier l'option `user` pour le lecteur respectif.

27.3.2 Commandes du système

La section suivante énumère les commandes les plus importantes en matière de récupération des informations du système, du traitement et du contrôle du réseau.

Informations système

`df [options] [répertoire]`

La commande `df` (disk free), si elle est utilisée sans options, affiche des informations sur l'espace disque total, l'espace disque actuellement utilisé et l'espace disponible sur tous les lecteurs montés. Si un répertoire est spécifié, les informations sont limitées au lecteur sur lequel se trouve ce répertoire.

`-h`
Affiche le nombre de blocs occupés en gigaoctets, mégaoctets ou kilo-octets, dans un format lisible.

`-T`
Type de système de fichiers (ext2, nfs, etc.).

du [options] [chemin]

Cette commande, si elle est exécutée sans paramètres, affiche l'espace disque total occupé par des fichiers et sous-répertoires dans le répertoire actuel.

-a
Affiche la taille de chaque fichier.

-h
Sortie dans le format lisible.

-s
Affiche seulement la taille totale calculée.

free [options]

La commande `free` affiche des informations concernant l'utilisation de la mémoire RAM et l'espace d'échange, en affichant le montant total et utilisé dans les deux catégories. Pour plus d'informations, consultez Section 30.1.6, « Commande free » (p. 500).

-b
Sortie en octets.

-k
Sortie en kilo-octets.

-m
Sortie en mégaoctets.

date [options]

Ce programme simple affiche l'heure système actuelle. S'il est exécuté en tant que `root`, il peut servir également à modifier l'heure du système. Les détails concernant le programme sont disponibles dans la page de manuel date(1).

Processus

`top [options]`

`top` offre un aperçu rapide des processus en cours d'exécution. Appuyez sur H pour accéder à une page qui explique brièvement les principales options permettant de personnaliser le programme.

`ps [options] [ID processus]`

Si elle est exécutée sans options, cette commande affiche un tableau de tous vos programmes ou processus - ceux que vous avez lancés. Les options de cette commande ne sont pas précédées d'un tiret.

aux

Affiche une liste détaillée de tous les processus, quel que soit le propriétaire.

`kill [options] ID processus`

Malheureusement, il est impossible parfois de fermer un programme normalement. Dans la plupart des cas, vous devez toujours être en mesure d'arrêter un tel programme en exécutant la commande `kill` et en spécifiant l'ID processus respectif (voir les commandes `top` et `ps`). `kill` envoie un signal *TERM* qui indique au programme de se fermer. Si cela n'aide pas, il est possible d'utiliser le paramètre suivant :

-9

Envoie un signal *KILL* au lieu d'un signal *TERM*, qui met fin au processus spécifié dans la plupart des cas.

`killall [options] nomprocessus`

Cette commande est similaire à la commande `kill`, mais utilise le nom du processus (au lieu de l'ID du processus) comme argument pour éliminer tous les processus portant le même nom.

Réseau

`ping [options] nom hôte ou adresse IP`

La commande `ping` est l'outil standard permettant de tester la fonctionnalité de base des réseaux TCP/IP. Elle envoie un petit paquet de données vers l'hôte cible en demandant une réponse immédiate. Si celui-ci fonctionne, `ping` affiche un message à cet effet, qui indique que le lien du réseau fonctionne.

`-c` ***`nombre`***
Détermine le nombre total de paquets à envoyer et se termine après leur envoi (par défaut, aucune limite n'est définie).

`-f`
flood ping : envoie autant de paquets de données que possible. C'est un moyen connu pour tester les réseaux, réservé à l'utilisateur `root`.

`-i` ***`valeur`***
Spécifie l'intervalle entre deux paquets de données en secondes (par défaut : une seconde).

`nslookup`

Le système de nom de domaine résout les noms de domaines en adresses IP. Cet outil permet d'envoyer des requêtes aux serveurs de noms (serveurs DNS).

`telnet [options] nom hôte ou adresse IP [port]`
Telnet est un protocole Internet qui vous permet de travailler sur des hôtes distants par le biais d'un réseau. telnet est également le nom d'un programme Linux qui utilise ce protocole pour activer des opérations sur des ordinateurs distants.

AVERTISSEMENT

N'utilisez pas telnet dans un réseau où les tiers sont susceptibles de vous « espionner ». En particulier sur Internet, vous pouvez utiliser les méthodes de transfert codées, telles que `ssh`, pour éviter tout risque d'utilisation malveillante d'un mot de passe (consultez les pages de manuel concernant `ssh`).

Divers

passwd [options] [nomutilisateur]

Cette commande permet aux utilisateurs de modifier à tout moment leurs propres mots de passe. L'administrateur `root` peut utiliser cette commande pour modifier le mot de passe de n'importe quel utilisateur dans le système.

su [options] [nomutilisateur]

La commande `su` permet de se loguer sous un nom d'utilisateur différent à partir d'une session en cours. Spécifiez un nom d'utilisateur et le mot de passe correspondant. Le mot de passe n'est pas requis de la part de l'utilisateur `root`. En effet, l'utilisateur `root` est autorisé à prendre l'identité de n'importe quel autre utilisateur. Lorsque vous utilisez la commande sans spécifier un nom d'utilisateur, vous êtes invité à entrer le mot de passe `root` et à basculer vers le superutilisateur (`root`).

-

Utilisez `su -` pour démarrer un shell de login pour l'utilisateur différent.

halt [options]

Pour éviter la perte de données, vous devez toujours utiliser ce programme pour arrêter votre système.

reboot [options]

Agit de la même façon que `halt`, excepté que le système exécute un redémarrage immédiat.

clear

Cette commande nettoie la partie visible de la console. Elle n'a pas d'options.

27.3.3 Pour plus d'informations

Il existe beaucoup plus de commandes que celles reprises dans ce chapitre. Pour obtenir des informations sur les autres commandes ou plus de détails, il est recommandé de lire l'ouvrage de O'Reilly intitulé *Linux in a Nutshell*.

27.4 L'éditeur vi

Les éditeurs de texte continuent à être utilisés pour de nombreuses tâches d'administration système, ainsi que pour la programmation. Dans le monde Unix, vi représente un éditeur qui offre des fonctions d'édition pratiques. Il est plus ergonomique que la plupart des autres éditeurs prenant en charge la souris.

27.4.1 Modes de fonctionnement

Fondamentalement, vi utilise trois modes de fonctionnement : le mode *insertion*, le mode *commande* et le mode *étendu*. Les touches ont différentes fonctions selon le mode utilisé. Au démarrage, vi est normalement défini en mode *commande*. Vous devez commencer par apprendre comment passer d'un mode à l'autre :

Du mode commande au mode insertion
Il existe de nombreuses possibilités, notamment la touche A pour ajouter, I pour insérer ou O pour créer une nouvelle ligne après la ligne actuelle.

Du mode insertion au mode commande
Appuyez sur la touche Échap pour quitter le mode *insertion*. Il n'est pas possible d'arrêter vi en mode *insertion* : il est donc important de prendre l'habitude d'appuyer sur Échap.

Du mode commande au mode étendu
Vous pouvez activer le mode *étendu* de vi en entrant deux points (:). Le mode *étendu* ou *ex* (pour « extended » - étendu) est comparable à un éditeur orienté ligne indépendant qui permet d'effectuer différentes tâches, des plus simples au plus complexes.

Du mode étendu au mode commande
Après avoir exécuté une commande en mode *étendu*, l'éditeur repasse automatiquement en mode *commande*. Si vous décidez de ne pas exécuter une commande en mode *étendu*, supprimez les deux points à l'aide de la touche ▯. L'éditeur repasse en mode *commande*.

Il n'est pas possible de passer directement du mode *insertion* au mode *étendu* sans d'abord passer par le mode *commande*.

Le programme vi, comme d'autres éditeurs, a sa propre procédure d'arrêt. Vous ne pouvez pas arrêter vi lorsqu'il est en mode *insertion*. Quittez d'abord le mode *insertion* en appuyant sur la touche Échap. Ensuite, vous avez deux options :

1. *Quitter sans enregistrer :* pour quitter l'éditeur sans enregistrer les modifications, entrez : – Q – ! en mode *commande*. Le point d'exclamation (!) indique à vi d'ignorer les modifications.

2. *Enregistrer et quitter :* il existe plusieurs possibilités pour enregistrer vos modifications et arrêter l'éditeur. En mode *commande*, utilisez Shift + Z + Z. Pour quitter le programme en enregistrant toutes les modifications à l'aide du mode *étendu*, entrez : – W – Q. En mode *étendu*, `w` représente « write » (écrire) et `q` « quit » (quitter).

27.4.2 vi en action

vi peut être utilisé comme un éditeur normal. En mode *insertion*, entrez ou supprimez du texte à l'aide des touches et Suppr. Utilisez les touches fléchées pour déplacer le curseur.

Toutefois, ces touches de contrôle génèrent souvent des problèmes, car il existe de nombreux types de terminaux qui utilisent des codes de touche spéciaux. C'est là que le mode *commande* entre en jeu. Appuyez sur Échap pour passer du mode *insertion* au mode *commande*. En mode *commande*, déplacez le curseur à l'aide des touches H, J, K et L. Ces touches ont les fonctions suivantes :

H
: se déplace d'un caractère vers la gauche

J
: passe à la ligne suivante

K
: remonte à la ligne précédente

L
: se déplace d'un caractère vers la droite

Les commandes en mode *commande* permettent plusieurs changements. Pour exécuter une commande plusieurs fois, il vous suffit d'entrer devant elle le nombre de fois où

elle sera répétée. Par exemple, entrez 5 L pour déplacer le curseur de cinq caractères vers la droite.

Pour obtenir une sélection des principales commandes, reportez-vous au Tableau 27.1, « Commandes simples de l'éditeur vi » (p. 450). Cette liste est loin d'être exhaustive. Des listes plus complètes sont disponibles dans la documentation présentée à la Section 27.4.3, « Pour plus d'informations » (p. 451).

Tableau 27.1 *Commandes simples de l'éditeur vi*

Échap	Passe en mode commande
I	Passe au mode insertion (les caractères apparaissent à la position courante du curseur)
A	Passe en mode insertion (les caractères sont insérés après la position actuelle du curseur)
Shift + A	Passe au mode insertion (les caractères sont ajoutés à la fin de la ligne)
Shift + R	Passe en mode remplacement (l'ancien texte est écrasé)
R	Remplace le caractère sous lequel se trouve le curseur
O	Passe au mode insertion (une nouvelle ligne est insérée après la ligne courante)
Shift + O	Passe au mode insertion (une nouvelle ligne est insérée avant la ligne courante)
X	Supprime le caractère actuel
D – D	Supprime la ligne actuelle
D – W	Supprime le mot courant jusqu'à la fin
C – W	Passe au mode insertion (le reste du mot courant est écrasé par les entrées suivantes)

U	Annule la dernière commande
Ctrl + R	Ré-applique la modification qui a été annulée
Shift + J	Rejoint la ligne suivante et la ligne actuelle
.	Répète la dernière commande

27.4.3 Pour plus d'informations

vi prend en charge une vaste gamme de commandes. Il permet d'utiliser des macros, des raccourcis, des mémoires tampons nommées, ainsi que de nombreuses autres fonctions pratiques. Une description détaillée de ces différentes options dépasserait le cadre de ce manuel. SUSE Linux est fourni avec vim (pour « vi improved »), une version améliorée de vi. Il existe de nombreuses sources d'informations pour cette application :

- vimtutor est un didacticiel interactif pour vim.
- Dans vim, entrez la commande `:help` pour obtenir de l'aide sur de nombreux sujets.
- Un manuel sur vim est disponible en ligne à l'adresse suivante : `http://www.truth.sk/vim/vimbook-OPL.pdf`.
- Les pages Web du projet vim sur le site `http://www.vim.org` proposent une grande variété d'informations récentes, de listes de diffusion et d'autres documentations.
- Plusieurs sources vim sont disponibles sur Internet : `http://www.selflinux.org/selflinux/html/vim.html`, `http://www.linuxgazette.com/node/view/9039` et `http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html`. Pour obtenir d'autres liens vers des didacticiels, reportez-vous à `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

IMPORTANT: Licence VIM

vim est un « caritaticiel » (« charityware » en anglais) : leurs auteurs ne font rien payer pour ce logiciel, mais vous demandent en contre-partie de faire un don financier pour un projet à but non lucratif. Ce projet fait appel à votre solidarité pour les enfants pauvres en Ouganda. Pour plus d'informations, connectez-vous aux sites `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` et `http://www.iccf.nl/`.

Amorçage et configuration d'un système Linux 28

L'amorçage d'un système Linux implique de nombreux composants. Ce chapitre décrit les principes sous-jacents et présente en détail les composants impliqués. Le concept de niveau d'exécution et la configuration du système SUSE avec `sysconfig` sont également abordés dans ce chapitre.

28.1 Le processus d'amorçage de Linux

Le processus d'amorçage de Linux se compose de plusieurs étapes, chacune représentée par un autre composant. La liste suivante résume brièvement le processus d'amorçage et présente tous les principaux composants impliqués.

1. **BIOS** Une fois l'ordinateur allumé, le BIOS initialise l'écran et le clavier, puis teste la mémoire principale. La machine n'accède jusque-là à aucun support de stockage de masse. Ensuite, les informations sur la date et l'heure actuelles ainsi que sur les périphériques les plus importants sont chargées à partir des valeurs CMOS. Lorsque le premier disque dur et sa géométrie sont reconnus, le contrôle du système passe du BIOS au chargeur d'amorçage.

2. **Chargeur d'amorçage** Le premier secteur de données de 512 octets du premier disque dur est chargé dans la mémoire principale et le *chargeur d'amorçage* qui réside au début de ce secteur prend la relève. Les commandes exécutées par le chargeur d'amorçage déterminent la partie restante du processus d'amorçage. Par conséquent, les 512 premiers octets du premier disque dur sont

appelés *MBR* (Master Boot Record - secteur d'amorçage principal). Le chargeur d'amorçage passe ensuite le contrôle au système d'exploitation, en l'occurrence le kernel Linux. Pour plus d'informations sur GRUB, le chargeur d'amorçage Linux, consultez le Chapitre 29, *Chargeur d'amorçage* (p. 471).

3. **Kernel et initramfs** Pour transmettre le contrôle du système, le chargeur d'amorçage charge le kernel et le système de fichiers initial basé sur la RAM (initramfs) dans la mémoire. Le contenu du système ramfs initial peut être utilisé par le kernel directement. Ce système contient un petit fichier exécutable appelé init qui traite le montage du système de fichiers racine réel. Dans les versions précédentes de SUSE Linux, ces tâches étaient traitées par initrd et linuxrc, respectivement. Pour plus d'informations sur initramfs, consultez la Section 28.1.1, « initramfs » (p. 454).

4. **init sur initramfs** Ce programme effectue toutes les actions nécessaires au montage du système de fichiers racine adéquat, notamment la mise en place des fonctionnalités du kernel pour le système de fichiers nécessaire et des pilotes de périphérique pour les contrôleurs de stockage de masse. Une fois le système de fichiers racine détecté, il est contrôlé afin de détecter les erreurs, puis monté. Si cette opération aboutit, le système initramfs est nettoyé et le programme init du système de fichiers racine est exécuté. Pour plus d'informations sur init, consultez la Section 28.1.2, « init sur initramfs » (p. 455).

5. **init** init prend en charge l'amorçage effectif du système par plusieurs niveaux qui fournissent des fonctionnalités différentes. Il est décrit à la Section 28.2, « Le processus init » (p. 457).

28.1.1 initramfs

initramfs est un petit système de fichiers que le kernel peut charger sur un disque virtuel. Il fournit un environnement Linux minimal qui permet d'exécuter des programmes avant le montage du système de fichiers racine réel. Cet environnement Linux minimal est chargé en mémoire par les routines du BIOS et n'a pas de configuration matérielle spécifique autre que suffisamment de mémoire. initramfs doit toujours fournir un fichier exécutable nommé init qui doit exécuter le programme d'initialisation proprement dit sur le système de fichiers racine afin de lancer le processus d'amorçage.

Avant que le système de fichiers racine réel puisse être monté et que le système d'exploitation puisse démarrer, le kernel a besoin des pilotes correspondants pour accéder

au périphérique sur lequel est situé le système de fichiers racine. Il peut s'agir de pilotes spéciaux pour certains types de disques durs ou de pilotes réseau permettant d'accéder à un système de fichiers réseau. Les modules nécessaires au système de fichiers racine peuvent être chargés par init sur initramfs. initramfs est disponible tout au long du processus d'amorçage. Tous les événements d'enfichage à chaud générés au cours de l'amorçage peuvent ainsi être traités.

Si vous devez changer le matériel (disques durs) sur un système installé et que ce matériel nécessite des pilotes différents dans le kernel au moment de l'amorçage, vous devez mettre à jour initramfs. Cette opération s'effectue comme avec son prédécesseur, initrd, en appelant `mkinitrd`. L'appel de `mkinitrd` sans argument crée initramfs. L'appel de `mkinitrd -R` crée initrd. Dans SUSE Linux, les modules à charger sont spécifiés par la variable `INITRD_MODULES` dans `/etc/sysconfig/kernel`. Après l'installation, cette variable adopte automatiquement la valeur correcte. Les modules sont chargés exactement dans l'ordre dans lequel ils apparaissent dans `INITRD_MODULES`. Cet aspect est très important, notamment en présence de plusieurs pilotes SCSI car sinon, les noms des disques durs seraient modifiés. En d'autres termes, il suffirait de charger uniquement les pilotes nécessaires pour accéder à ce système de fichiers racine. Cependant, tous les pilotes SCSI nécessaires à l'installation sont chargés au moyen d'initramfs ou d'initrd car un chargement ultérieur risquerait de poser problème.

IMPORTANT: Mise à jour d'initramfs ou d'initrd

Le chargeur d'amorçage charge initramfs ou initrd de la même manière que le kernel. Il est inutile de réinstaller GRUB après la mise à jour d'initramfs ou d'initrd car GRUB recherche le fichier correct dans le répertoire lors de l'amorçage.

28.1.2 init sur initramfs

L'objectif principal d'init sur initramfs est de préparer le montage du système de fichiers racine réel ainsi que son accès. En fonction de la configuration actuelle de votre système, init est responsable des tâches suivantes.

Chargement des modules du kernel

En fonction de votre configuration matérielle, des pilotes spéciaux peuvent être nécessaires pour accéder aux composants matériels de votre ordinateur (le composant le plus important étant votre disque dur). Pour accéder au système de fichiers racine final, le kernel doit charger les pilotes corrects du système de fichiers.

Gestion des configurations RAID et LVM
Si vous avez configuré votre système pour que le système de fichiers racine soit contenu sous RAID ou LVM, init configure LVM ou RAID pour permettre l'accès ultérieur au système de fichiers racine. Pour plus d'informations sur RAID, consultez la Section 2.3, « Configuration de Soft RAID » (p. 70). Pour plus d'informations sur LVM, consultez la Section 2.2, « Configuration du gestionnaire de volumes logiques (LVM) » (p. 62).

Gestion de la configuration réseau
Si vous avez configuré votre système pour qu'il utilise un système de fichiers racine monté sur un réseau (monté via NFS), init doit s'assurer que les pilotes réseau correspondants sont chargés et qu'ils sont configurés pour autoriser l'accès au système de fichiers racine.

Lorsque init est appelé au cours de l'amorçage initial dans le cadre du processus d'installation, ses tâches diffèrent de celles mentionnées précédemment :

Recherche du support d'installation
Lorsque vous démarrez le processus d'installation, votre machine charge un kernel d'installation et un initrd spécial avec le programme d'installation de YaST à partir du support d'installation. Le programme d'installation de YaST, qui est exécuté dans un système de fichiers RAM, doit disposer d'informations sur l'emplacement réel du support d'installation pour y accéder et installer le système d'exploitation.

Reconnaissance matérielle et chargement des modules de kernel correspondants
Comme l'indique la Section 28.1.1, « initramfs » (p. 454), le processus d'amorçage démarre avec un ensemble réduit de pilotes qui peuvent être utilisés avec la plupart des configurations matérielles. init démarre un processus de recherche matérielle qui détermine l'ensemble des pilotes adaptés à votre configuration matérielle. Ces valeurs sont ensuite écrites dans `INITRD_MODULES` dans `/etc/sysconfig/kernel` pour permettre à tout processus d'amorçage ultérieur d'utiliser un initrd personnalisé. Au cours du processus d'installation, init charge cet ensemble de modules.

Chargement du système d'installation et système de secours
Dès que le matériel a été correctement reconnu et que les pilotes correspondants ont été chargés, init démarre le système d'installation qui contient le programme d'installation de YaST proprement dit ou le système de secours.

Démarrage de YaST
Pour finir, init démarre YaST, qui lance l'installation des paquetages et la configuration du système.

28.2 Le processus init

Le programme init est le processus portant le numéro de processus 1. Il est responsable de l'initialisation du système de la manière requise. init joue un rôle spécial. Il est démarré directement par le kernel et résiste au signal 9 qui, en règle générale, détruit les processus. Tous les autres programmes sont soit démarrés directement par init, soit par l'un de ses processus enfants.

init est configuré de manière centralisée dans le fichier `/etc/inittab` où les *niveaux d'exécution* sont définis (consultez la Section 28.2.1, « Niveaux d'exécution » (p. 457)). Ce fichier indique également les services et les démons disponibles dans chacun des niveaux. En fonction des entrées de `/etc/inittab`, plusieurs scripts sont exécutés par init. Pour des raisons de clarté, ces scripts, appelés *scripts init*, résident tous dans le répertoire `/etc/init.d` (consultez la Section 28.2.2, « Scripts d'initialisation » (p. 460)).

Le processus de démarrage et d'arrêt du système est intégralement géré par init. De ce point de vue, le kernel peut être considéré comme un processus d'arrière-plan dont la tâche est de prendre en charge tous les autres processus et de régler l'horloge de l'unité centrale et l'accès matériel en fonction des requêtes en provenance d'autres programmes.

28.2.1 Niveaux d'exécution

Sous Linux, les *niveaux d'exécution* définissent le mode de démarrage du système et les services disponibles sur le système en cours d'exécution. Après l'amorçage, le système démarre conformément à la ligne `initdefault` du fichier `/etc/inittab`. Il s'agit généralement du niveau d'exécution `3` ou `5`. Voir Tableau 28.1, « Niveaux d'exécution disponibles » (p. 458). Il est également possible de spécifier le niveau d'exécution au moment de l'amorçage (à l'invite d'amorçage, par exemple). Tous les paramètres qui ne sont pas directement évalués par le kernel sont transmis à init.

Tableau 28.1 Niveaux d'exécution disponibles

Niveau d'exécution	Description
0	Arrêt du système
S	Mode mono-utilisateur ; à partir de l'invite d'amorçage, uniquement avec disposition de clavier américaine
1	Mode mono-utilisateur
2	Mode multi-utilisateur local sans réseau distant (NFS, etc.)
3	Mode multi-utilisateur intégral avec réseau
4	Non utilisé
5	Mode multi-utilisateur intégral avec réseau et gestionnaire d'affichage X (KDM, GDM ou XDM)
6	Redémarrage du système

IMPORTANT: Éviter le niveau d'exécution 2 avec une partition /usr montée par NFS

Vous ne devez pas utiliser le niveau d'exécution 2 si votre système monte la partition `/usr` via NFS. Le répertoire `/usr` contient des programmes importants essentiels au fonctionnement correct du système. Comme le service NFS n'est pas disponible au niveau d'exécution 2 (mode multi-utilisateur local sans réseau distant), le système serait considérablement limité à de nombreux égards.

Pour modifier le niveau d'exécution alors que le système est en cours d'exécution, entrez `init` et le numéro correspondant comme argument. Seul l'administrateur système est autorisé à effectuer cette opération. La liste suivante résume les principales commandes dans la zone du niveau d'exécution.

`init 1` ou `shutdown now`
Le système passe en *mode mono-utilisateur*. Ce mode est utilisé pour la maintenance du système et les tâches d'administration.

`init 3`
Tous les programmes et services essentiels (notamment réseau) sont démarrés et les utilisateurs standard sont autorisés à se loguer et à utiliser le système sans environnement graphique.

`init 5`
L'environnement graphique est activé. Il peut s'agir d'un des bureaux (GNOME ou KDE) ou de tout gestionnaire de fenêtres.

`init 0` ou `shutdown -h now`
Le système s'arrête.

`init 6` ou `shutdown -r now`
Le système s'arrête et redémarre.

Le niveau d'exécution `5` est le niveau d'exécution par défaut dans toutes les installations standard SUSE Linux. Les utilisateurs sont invités à se loguer avec une interface graphique. Si le niveau d'exécution par défaut est `3`, le système X Window doit être configuré correctement, comme le décrit le Chapitre 35, *Système X Window* (p. 563), avant que le niveau d'exécution puisse passer à `5`. Dans ce cas, vérifiez le bon fonctionnement du système en entrant `init 5` . Si tout fonctionne comme prévu, vous pouvez utiliser YaST pour définir sur `5` le niveau d'exécution par défaut.

AVERTISSEMENT: Erreurs /etc/inittab susceptibles d'altérer l'amorçage du système

Si `/etc/inittab` est endommagé, le système risque de ne pas démarrer correctement. Par conséquent, soyez extrêmement vigilant lorsque vous modifiez `/etc/inittab` et conservez toujours une sauvegarde d'une version intacte. Pour réparer d'éventuels dommages, essayez d'entrer `init=/bin/sh` après le nom du kernel à l'invite d'amorçage pour démarrer directement dans un shell. Ensuite, autorisez l'accès en écriture sur votre système de fichiers racine à l'aide de la commande `mount -o remount,rw /` et remplacez `/etc/inittab` par votre version de sauvegarde à l'aide de `cp`. Pour éviter les erreurs du système de fichiers, autorisez l'accès en lecture seule uniquement à votre

système de fichiers racine avant de procéder au redémarrage à l'aide de la commande `mount -o remount,ro /` .

Généralement, deux événements se produisent lorsque vous changez de niveau d'exécution. Tout d'abord, les scripts d'arrêt du niveau d'exécution en cours sont lancés, ce qui entraîne la fermeture de certains programmes essentiels au niveau d'exécution en cours. Ensuite, des scripts de démarrage du nouveau niveau d'exécution sont démarrés. Dans la plupart des cas, un certain nombre de programmes sont démarrés. Voici par exemple ce qui se produit lors du passage du niveau d'exécution 3 à 5 :

1. L'administrateur (`root`) demande à init de passer à un autre niveau d'exécution en entrant `init 5` .

2. init consulte son fichier de configuration (`/etc/inittab`) et détermine qu'il doit démarrer `/etc/init.d/rc` avec le nouveau niveau d'exécution comme paramètre.

3. La commande `rc` appelle alors tous les scripts d'arrêt du niveau d'exécution actuel, mais uniquement ceux qui ne sont associés à aucun script de démarrage dans le nouveau niveau d'exécution. Dans cet exemple, il s'agit de tous les scripts situés dans `/etc/init.d/rc3.d` (l'ancien niveau d'exécution était 3) et qui commencent par un `K`. Le nombre qui suit le `K` indique l'ordre de démarrage car certaines dépendances doivent être prises en compte.

4. Les derniers éléments à démarrer sont les scripts de démarrage du nouveau niveau d'exécution. Il sont situés, dans cet exemple, dans `/etc/init.d/rc5.d` et commencent par un `S`. La même procédure concernant l'ordre de démarrage s'applique ici.

Lorsque vous passez au même niveau d'exécution que le niveau d'exécution actuel, init vérifie uniquement `/etc/inittab` afin d'y détecter d'éventuelles modifications et lance les étapes correspondantes, par exemple, pour démarrer un `getty` sur une autre interface.

28.2.2 Scripts d'initialisation

Il existe deux types de scripts dans `/etc/init.d`:

Les scripts exécutés directement par init

C'est uniquement le cas au cours du processus d'amorçage ou si un arrêt immédiat du système a lieu (panne de courant ou si un utilisateur appuie sur les touches Ctrl + Alt + Suppr). L'exécution de ces scripts est définie dans `/etc/inittab`.

Les scripts exécutés indirectement par init

Ces scripts sont exécutés lors d'un changement du niveau d'exécution et appellent toujours le script maître `/etc/init.d/rc`, qui garantit l'ordre correct des scripts correspondants.

Tous les scripts sont situés dans `/etc/init.d`. Les scripts de changement du niveau d'exécution se trouvent également à cet emplacement, mais sont appelés par des liens symboliques à partir d'un des sous-répertoires (`/etc/init.d/rc0.d` à `/etc/init.d/rc6.d`), ceci pour des raisons de clarté et pour éviter les scripts en double s'ils sont utilisés dans plusieurs niveaux d'exécution. Comme chaque script peut être exécuté comme un script de démarrage et d'arrêt, ces scripts doivent savoir interpréter les paramètres `start` et `stop`. Ils doivent également reconnaître les options `restart`, `reload`, `force-reload` et `status`. Ces différentes options sont décrites dans le Tableau 28.2, « Options possibles des scripts d'initialisation » (p. 461). Les scripts exécutés directement par init ne disposent pas de ces liens. Ils sont exécutés indépendamment à partir du niveau d'exécution, si nécessaire.

Tableau 28.2 *Options possibles des scripts d'initialisation*

Option	Description
`start`	Démarre le service.
`stop`	Arrête le service.
`restart`	Si le service est en cours d'exécution, cette option l'arrête, puis le redémarre. S'il n'est pas en cours d'exécution, elle le démarre.
`reload`	Recharge la configuration sans arrêter et redémarrer le service.

Option	Description
`force-reload`	Recharge la configuration si le service prend cette opération en charge. Sinon, effectue la même action que l'option `restart`.
`status`	Affiche l'état actuel du service.

Des liens dans chaque sous-répertoire propre au niveau d'exécution permettent d'associer des scripts à différents niveaux d'exécution. Lors de l'installation ou de la désinstallation des paquetages, ces liens sont ajoutés et supprimés à l'aide du programme insserv (ou du script `/usr/lib/lsb/install_initd` qui appelle ce programme). Pour plus d'informations, consultez la page du manuel sur insserv(8).

Une brève introduction aux scripts d'amorçage et d'arrêt lancés en premier ou en dernier lieu, respectivement, suit ainsi qu'une explication du script de maintenance.

`boot`

Exécuté lors du démarrage du système directement à l'aide d'init. Il est indépendant du niveau d'exécution choisi et est exécuté une seule fois. Les systèmes de fichiers `proc` et `pts` sont montés et le démon blogd de journalisation des informations d'amorçage est activé. Si le système est amorcé pour la première fois après une mise à jour ou une installation, la configuration initiale du système est démarrée.

Le démon blogd est un service démarré en tout premier lieu par boot et rc. Il est arrêté dès la fin des actions déclenchées par les scripts ci-dessus (exécutant un certain nombre de sous-scripts, par exemple). Le démon blogd écrit toutes les sorties d'écran dans le fichier journal `/var/log/boot.msg`, mais uniquement si et lorsque `/var` est monté en lecture-écriture. Sinon, blogd met en tampon toutes les données d'écran jusqu'à ce que `/var` soit disponible. Pour plus d'informations, consultez la page du manuel sur blogd(8).

Le script `boot` est également chargé du démarrage de tous les scripts situés dans `/etc/init.d/boot.d` et dont le nom commence par `S`. Les systèmes de fichiers sont contrôlés et les périphériques de bouclage (loop) sont configurés, si nécessaire. L'horloge système est également définie. Si une erreur survient au cours du contrôle et de la réparation automatiques du système de fichiers, l'administrateur système peut intervenir après avoir entré le mot de passe root. Le script `boot.local` est exécuté en dernier lieu.

boot.local
: Entrez ici les commandes supplémentaires à exécuter au démarrage avant de changer de niveau d'exécution. Ce script est comparable au fichier `AUTOEXEC.BAT` sur les systèmes DOS.

boot.setup
: Ce script est exécuté lors du passage du mode mono-utilisateur à tout autre niveau d'exécution. Il est chargé d'un certain nombre de paramétrages de base, tels que la disposition du clavier et l'initialisation des consoles virtuelles.

halt
: Ce script est uniquement exécuté lors du passage au niveau d'exécution 0 ou 6. Ici, il est exécuté comme équivalent de `halt` ou de `reboot`. L'arrêt ou le redémarrage du système dépend de la manière dont `halt` est appelé.

rc
: Ce script appelle les scripts d'arrêt appropriés du niveau d'exécution actuel et les scripts de démarrage du nouveau niveau d'exécution sélectionné.

Vous pouvez créer vos propres scripts et les intégrer facilement dans le modèle décrit ci-dessus. Pour plus d'informations sur le formatage, l'assignation de noms et l'organisation des scripts personnalisés, consultez les spécifications établies par les normes LSB et les pages du manuel sur `init`, `init.d` et `insserv`. Consultez également les pages du manuel sur `startproc` et `killproc`.

AVERTISSEMENT: Scripts d'initialisation défectueux susceptibles d'arrêter votre système

Les scripts init défectueux peuvent bloquer votre machine. Modifiez ces scripts avec le plus grand soin et, si possible, soumettez-les à des tests importants dans un environnement multi-utilisateur. Vous trouverez des informations utiles sur les scripts init à la Section 28.2.1, « Niveaux d'exécution » (p. 457).

Pour créer un script init personnalisé pour un programme ou un service donné, utilisez comme modèle le fichier `/etc/init.d/skeleton`. Enregistrez une copie de ce fichier sous son nouveau nom et modifiez les noms de programme et de fichier, les chemins correspondants, ainsi que les autres informations nécessaires. Vous pouvez également améliorer le script en y ajoutant vos propres parties afin que les actions correctes soient déclenchées par la procédure d'initialisation.

Le bloc `INIT INFO` situé au début du script est une partie obligatoire qui doit être modifiée. Voir Exemple 28.1, « Bloc INIT INFO minimal » (p. 464).

Exemple 28.1 *Bloc INIT INFO minimal*

```
### BEGIN INIT INFO
# Provides:          TOTO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Démarre TOTO pour autoriser XY et fournir YZ
### END INIT INFO
```

Sur la première ligne du bloc `INFO`, après `Provides:`, indiquez le nom du programme ou service contrôlé par ce script init. Sur les lignes `Required-Start:` et `Required-Stop:`, indiquez tous les services qui doivent être démarrés ou arrêtés avant le démarrage ou l'arrêt du service même. Ces informations sont utilisées ultérieurement pour générer la numérotation des noms de script tels qu'ils figurent dans les répertoires de niveau d'exécution. Après `Default-Start:` et `Default-Stop:`, indiquez les niveaux d'exécution dans lesquels le service doit automatiquement être démarré ou arrêté. Enfin, pour `Description:`, fournissez une brève description du service en question.

Pour créer des liens à partir des répertoires de niveau d'exécution (`/etc/init.d/rc?.d/`) vers les scripts correspondants dans `/etc/init.d/`, entrez la commande `insserv` *`nouveau nom de script`* . Le programme insserv évalue l'en-tête `INIT INFO` pour créer les liens nécessaires aux scripts de démarrage et d'arrêt dans les répertoires de niveau d'exécution (`/etc/init.d/rc?.d/`). Le programme s'occupe également de l'ordre correct de démarrage et d'arrêt de chaque niveau d'exécution en incluant les numéros nécessaires dans les noms figurant dans ces liens. Si vous préférez qu'un outil graphique crée ces liens, utilisez l'éditeur de niveaux d'exécution fourni par YaST, conformément aux instructions de la Section 28.2.3, « Configuration des services système (niveau d'exécution) avec YaST » (p. 465).

Si un script déjà présent dans `/etc/init.d/` doit être intégré au modèle de niveau d'exécution existant, créez les liens dans les répertoires du niveau d'exécution directement avec insserv ou en activant le service correspondant dans l'éditeur de niveaux d'exécution de YaST. Les modifications sont appliquées lors du redémarrage suivant. Le nouveau service est démarré automatiquement.

Ne définissez pas ces liens manuellement. Si une information est incorrecte dans le bloc `INFO`, des problèmes surviennent lorsque `insserv` est exécuté ultérieurement pour un autre service.

28.2.3 Configuration des services système (niveau d'exécution) avec YaST

Après avoir démarré ce module YaST en sélectionnant *YaST* → *Système* → *Services système (niveau d'exécution)*, vous voyez apparaître la liste de tous les services disponibles et l'état actuel de chaque service (désactivé ou activé). Choisissez d'utiliser le module en *mode simple* ou en *mode Experts*. Le*mode simple* par défaut suffit dans la plupart des cas. La colonne de gauche indique le nom du service, la colonne du milieu renseigne sur l'état actuel et la colonne de droite donne une brève description. En ce qui concerne le service sélectionné, une description plus détaillée apparaît au bas de la fenêtre. Pour activer un service, sélectionnez-le dans le tableau et cliquez sur *Activer*. Procédez de même pour désactiver un service.

Figure 28.1 *Services système (niveau d'exécution)*

Pour effectuer un contrôle détaillé sur les niveaux d'exécution dans lesquels un service est démarré ou arrêté, ou pour modifier le niveau d'exécution par défaut, sélectionnez d'abord le *mode Experts*. Le niveau d'exécution par défaut actuel ou « initdefault »

(niveau d'exécution dans lequel le système démarre par défaut) est affiché en haut. En règle générale, le niveau d'exécution par défaut d'un système SUSE Linux est le niveau d'exécution 5 (mode multi-utilisateur intégral avec réseau et X). Le niveau d'exécution 3 (mode multi-utilisateur intégral avec réseau) offre une alternative appropriée.

Cette boîte de dialogue YaST permet de sélectionner l'un des niveaux d'exécution (répertoriés dans le Tableau 28.1, « Niveaux d'exécution disponibles » (p. 458)) comme nouveau niveau d'exécution par défaut. Utilisez également le tableau de cette fenêtre pour activer ou désactiver un à un des services et des démons. Ce tableau liste les services et les démons disponibles, indique s'ils sont actuellement activés sur votre système et, si c'est le cas, pour quels niveaux d'exécution. Après avoir sélectionné l'une des lignes avec la souris, cochez les cases représentant les niveaux d'exécution (*B*, *0*, *1*, *2*, *3*, *5*, *6* et *S*) pour définir les niveaux d'exécution dans lesquels le service ou le démon sélectionné doit s'exécuter. Au départ, le niveau d'exécution 4 n'est pas défini pour permettre la création d'un niveau d'exécution personnalisé. Une brève description du service ou du démon sélectionné est fournie sous le tableau.

À l'aide des options *Démarrer/Arrêter/Actualiser*, indiquez si un service doit être activé. L'option *Actualiser l'état* vérifie l'état actuel. L'option *Définir/Remettre à zéro* permet d'appliquer les modifications au système ou de restaurer les paramètres en vigueur avant le démarrage de l'éditeur de niveaux d'exécution. Sélectionnez *Terminer* pour enregistrer les nouveaux paramètres sur le disque.

AVERTISSEMENT: Paramètres de niveau d'exécution incorrects susceptibles d'endommager votre système

Le système peut devenir instable du fait de paramètres de niveau d'exécution incorrects. Avant d'appliquer les modifications, assurez-vous absolument que vous en connaissez les conséquences.

28.3 Configuration système via /etc/sysconfig

La configuration principale de SUSE Linux est contrôlée par les fichiers de configuration situés dans `/etc/sysconfig`. Chaque fichier de `/etc/sysconfig` est uniquement lu par les scripts auxquels il correspond. Ainsi, les paramètres réseau, par exemple, doivent uniquement être analysés par les scripts relatifs au réseau. De nombreux autres

fichiers de configuration système sont générés conformément aux paramètres de /etc/sysconfig. Cette tâche est effectuée par SuSEconfig. Par exemple, si vous modifiez la configuration réseau, SuSEconfig risque d'apporter des modifications au fichier /etc/host.conf également, puisqu'il s'agit d'un des fichiers relatifs à la configuration du réseau. Ce concept vous permet d'effectuer des modifications de base à votre configuration sans avoir à redémarrer le système.

Deux méthodes permettent de modifier la configuration système. Utilisez l'éditeur sysconfig de YaST ou modifiez manuellement les fichiers de configuration.

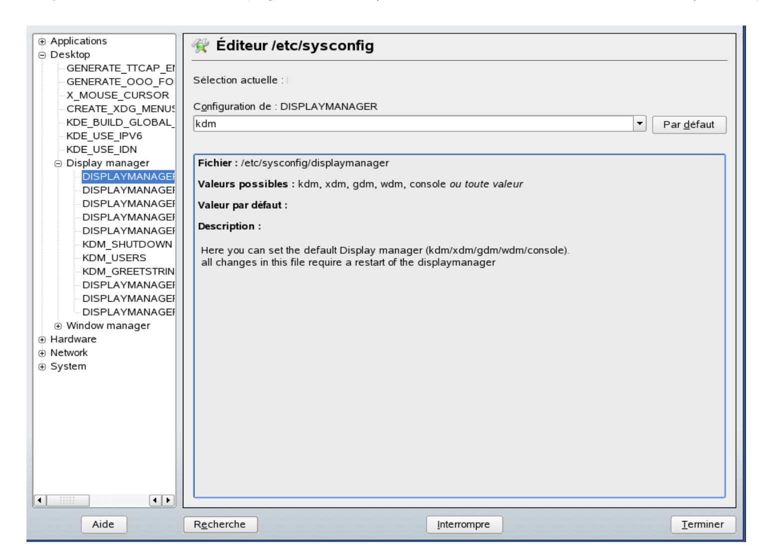
28.3.1 Modification de la configuration système à l'aide de l'éditeur sysconfig de YaST

L'éditeur sysconfig de YaST offre une interface client conviviale pour configurer le système. Sans connaître l'emplacement réel de la variable de configuration que vous devez modifier, utilisez simplement la fonction de recherche intégrée de ce module et modifiez la valeur de la variable de configuration. YaST se charge ensuite d'appliquer ces modifications, de mettre à jour les configurations qui dépendent des valeurs définies dans sysconfig et de redémarrer les services.

AVERTISSEMENT: La modification des fichiers de /etc/sysconfig/* peut endommager votre installation

Ne modifiez pas les fichiers /etc/sysconfig si vous ne disposez pas de l'expérience et des connaissances suffisantes. Cette opération risquerait d'endommager sérieusement votre système. Les fichiers situés dans /etc/sysconfig comprennent un bref commentaire sur chaque variable, qui explique leur effet réel.

Figure 28.2 *Configuration système à l'aide de l'éditeur sysconfig*



La boîte de dialogue sysconfig de YaST est divisée en trois parties. La partie gauche de la boîte de dialogue affiche une vue arborescente des variables configurables. Lorsque vous sélectionnez une variable, la partie droite affiche la sélection et le paramètre actuels de cette variable. En dessous, une troisième fenêtre affiche une brève description du rôle de la variable, des valeurs possibles, de la valeur par défaut, ainsi que le fichier de configuration dont est issue cette variable. Cette boîte de dialogue fournit également des informations sur le script de configuration qui est exécuté après la modification de la variable et le service qui est démarré à la suite cette opération. YaST vous invite à confirmer les modifications et indique les scripts qui sont exécutés lorsque vous fermez la boîte de dialogue en sélectionnant *Terminer*. Sélectionnez également les services et les scripts à ignorer à ce stade afin qu'ils soient démarrés ultérieurement. YaST applique toutes les modifications automatiquement et redémarre tous les services impliqués afin que les modifications prennent effet.

28.3.2 Modification manuelle de la configuration système

Pour modifier manuellement la configuration système, procédez comme suit :

1 Devenez utilisateur `root`.

2 Mettez le système en mode mono-utilisateur unique (niveau d'exécution 1) avec `init 1`.

3 Au besoin, modifiez les fichiers de configuration avec l'éditeur de votre choix.

Si vous n'utilisez pas YaST pour modifier les fichiers de configuration de `/etc/sysconfig`, assurez-vous que les valeurs de variable vides sont représentées par des guillemets doubles (`KEYTABLE=""`) et que les valeurs comportant des espaces sont encadrées par des guillemets. Les valeurs composées d'un seul mot ne doivent pas être placées entre guillemets.

4 Exécutez `SuSEconfig` pour vous assurer que les modifications prennent effet.

5 Rétablissez le niveau d'exécution antérieur du système avec une commande comme `init` *`niveau exécution par défaut`*. Remplacez *`niveau exécution par défaut`* par le niveau d'exécution par défaut du système. Choisissez `5` si vous souhaitez revenir au mode multi-utilisateur intégral avec réseau et X. Choisissez `3` si vous préférez travailler en mode multi-utilisateur intégral sans réseau.

Cette procédure est surtout utile lors de la modification des paramètres à l'échelle du système, notamment la configuration réseau. Les modifications mineures n'imposent pas de passer en mode mono-utilisateur, mais vous pouvez toujours le faire pour être absolument sûr que tous les programmes concernés sont correctement redémarrés.

ASTUCE: Paramétrage de la configuration automatique du système

Pour désactiver la configuration automatique du système par SuSEconfig, attribuez la valeur `no` à la variable `ENABLE_SUSECONFIG` dans `/etc/sysconfig/suseconfig`. Ne désactivez pas SuSEconfig si vous souhaitez utiliser la prise en charge de l'installation SUSE. Il est également possible de désactiver partiellement la configuration automatique.

---

29 Chargeur d'amorçage

Ce chapitre présente le mode de configuration de GRUB, le chargeur d'amorçage utilisé dans SUSE Linux. Un module YaST spécial vous permet d'effectuer tous les paramétrages. Si la fonction d'amorçage dans Linux ne vous est pas familière, lisez les sections suivantes ; elles vous fourniront des informations de base. Ce chapitre décrit également certains problèmes souvent rencontrés lorsque vous procédez à un amorçage à l'aide de GRUB et propose des solutions pour y remédier.

Ce chapitre s'attache à la gestion de l'amorçage et à la configuration du chargeur d'amorçage GRUB. L'ensemble de la procédure d'amorçage est décrite au Chapitre 28, *Amorçage et configuration d'un système Linux* (p. 453). Un chargeur d'amorçage constitue l'interface entre votre ordinateur (BIOS) et le système d'exploitation (SUSE Linux). La configuration du chargeur d'amorçage a une incidence directe sur le mode de démarrage du système d'exploitation.

Les termes suivants apparaissent fréquemment dans ce chapitre et il peut être utile d'en fournir une définition :

Secteur d'amorçage principal

La structure du MBR (Master Boot Record - secteur d'amorçage principal) est définie selon une convention indépendante du type de système d'exploitation. Les 446 premiers octets sont réservés au code programme. Ils stockent généralement le programme du chargeur d'amorçage, en l'occurrence, GRUB. Les 64 octets suivants fournissent de l'espace pour une table de partitions avec quatre entrées au maximum (consultez la section intitulée « Types de partitions » (Chapitre 1, *Installation avec YaST*, ↑Démarrage)). La table de partitions contient des informations sur le partitionnement du disque dur et le type de système de fichiers utilisé. Cette table est indis-

pensable au système d'exploitation pour la gestion du disque dur. Les deux derniers octets du MBR doivent comporter un « nombre magique » statique (AA55). Si un MBR contient une valeur différente, le BIOS, ainsi que tous les systèmes d'exploitation PC, le considèrent comme non valide.

Secteurs d'amorçage

Les secteurs d'amorçage sont les premiers secteurs des partitions du disque dur, à l'exception de la partition étendue qui sert principalement de « conteneur » pour d'autres partitions. Ces secteurs d'amorçage disposent de 512 octets d'espace, destinés au code servant à amorcer un système d'exploitation installé dans la partition correspondante. Cela s'applique aux secteurs d'amorçage des partitions au format DOS, Windows et OS/2, qui contiennent également d'importantes données de base concernant le système de fichiers. En revanche, les secteurs d'amorçage des partitions Linux sont, à l'origine, vides après l'installation d'un système de fichiers. Par conséquent, une partition Linux *ne peut pas s'amorcer seule*, même si elle contient un kernel et un système de fichiers racine valide. Un secteur d'amorçage avec du code valide pour l'amorçage du système présente le même numéro magique, dans ses deux derniers octets, que le MBR (`AA55`).

29.1 Gestion de l'amorçage

Si l'on considère le cas de figure le plus simple (ordinateur où est installé un seul système d'exploitation), la gestion de l'amorçage s'effectue de la manière décrite ci-dessus. Si plusieurs systèmes d'exploitation sont installés sur un même ordinateur, vous disposez des options suivantes :

Amorçage de systèmes supplémentaires à partir d'un support externe

L'un des systèmes d'exploitation est amorcé à partir du disque dur. Les autres systèmes d'exploitation sont amorcés à l'aide d'un gestionnaire d'amorçage installé sur un support externe (disquette, CD, support de stockage USB).

Installation d'un gestionnaire d'amorçage dans le MBR

Un gestionnaire d'amorçage permet l'installation simultanée, ainsi que l'utilisation alternée, de plusieurs systèmes d'exploitation sur un même ordinateur. Les utilisateurs peuvent choisir le système à démarrer au cours du processus d'amorçage. Pour passer à un autre système d'exploitation, réamorcez l'ordinateur. Cette opération n'est possible que si le gestionnaire d'amorçage sélectionné est compatible avec les

systèmes d'exploitation installés. GRUB est le gestionnaire d'amorçage utilisé sous SUSE Linux.

29.2 Sélection d'un chargeur d'amorçage

Par défaut, le chargeur d'amorçage GRUB est utilisé sous SUSE Linux. Toutefois, dans certains cas, et pour des configurations matérielles et logicielles particulières, LILO peut s'avérer plus adapté. La mise à jour d'une ancienne version de SUSE Linux qui utilise LILO entraîne également l'installation de LILO.

Pour obtenir des informations sur l'installation et la configuration de LILO, entrez le mot-clé LILO dans la base de données de support ou accédez au fichier `/usr/share/doc/packages/lilo`.

29.3 Amorçage à l'aide de GRUB

GRUB (Grand Unified Bootloader) comprend deux niveaux : le premier (stage1) est écrit sur 512 octets dans le MBR, ou dans le secteur d'amorçage d'une disquette ou d'une partition du disque dur. Ensuite, le programme charge le niveau 2 (stage2). Il contient le code de programme proprement dit. La seule tâche qu'effectue le premier niveau consiste à charger le deuxième niveau du chargeur d'amorçage.

Le niveau stage2 permet d'accéder à des systèmes de fichiers. Actuellement, Ext2, Ext3, ReiserFS, Minix et le système de fichiers DOS FAT utilisé par Windows sont pris en charge. Dans une certaine mesure, JFS, XFS, et UFS et FFS (utilisés par les systèmes BSD) sont également pris en charge. Depuis la version 0.95, GRUB est également capable d'effectuer un amorçage à partir d'un CD ou d'un DVD contenant un système de fichiers ISO 9660, conforme à la spécification « El Torito ». Avant même l'amorçage du système, GRUB peut accéder aux systèmes de fichiers des lecteurs de disque BIOS pris en charge (disquettes ou disques durs, et lecteurs de CD et de DVD détectés par le BIOS). C'est pourquoi il est inutile de réinstaller le gestionnaire d'amorçage si vous modifiez le fichier de configuration GRUB (`menu.lst`). Lors de l'amorçage du système, GRUB recharge le fichier de menu contenant les chemins (et les données de partition) valides du kernel ou du disque virtuel initial (`initrd`), puis il repère ces fichiers.

La configuration proprement dite de GRUB repose sur les trois fichiers suivants :

`/boot/grub/menu.lst`

Ce fichier contient toutes les informations relatives aux partitions ou aux systèmes d'exploitation qui peuvent être amorcés avec GRUB. Sans ces informations, le système d'exploitation ne peut pas prendre le contrôle du système.

`/boot/grub/device.map`

Ce fichier traduit les noms de périphérique écrits en notation GRUB et BIOS en noms de périphérique Linux.

`/etc/grub.conf`

Ce fichier contient les paramètres et options dont le shell GRUB a besoin pour installer correctement le chargeur d'amorçage.

Vous contrôlez GRUB de différentes manières. Vous sélectionnez les entrées d'amorçage d'une configuration existante depuis le menu graphique de l'écran de démarrage. La configuration est chargée à partir du fichier `menu.lst`.

GRUB permet de modifier tous les paramètres d'amorçage avant de lancer l'amorçage. Vous pouvez ainsi corriger les erreurs commises lors de la modification du fichier de menu, par exemple. Les commandes d'amorçage peuvent également être entrées de manière interactive, à l'aide d'une sorte d'invite de saisie (consultez la section intitulée « Modification des entrées de menu au cours de la procédure d'amorçage » (p. 479)). GRUB permet aussi de déterminer l'emplacement du kernel et du fichier `initrd` avant de lancer l'amorçage. Ainsi, vous pouvez même amorcer un système d'exploitation installé qui ne figure pas dans la configuration du chargeur d'amorçage.

Le *shell GRUB* fournit une fonction d'émulation de GRUB dans le système installé. Vous pouvez l'utiliser pour installer GRUB ou pour tester de nouveaux paramètres avant de les appliquer. (voir Section 29.3.4, « Shell GRUB » (p. 482)).

29.3.1 Menu d'amorçage GRUB

L'écran graphique de démarrage où figure le menu d'amorçage repose sur le fichier de configuration de GRUB, `/boot/grub/menu.lst` ; ce dernier contient toutes les

informations relatives aux partitions ou systèmes d'exploitation qui peuvent être amorcés à partir du menu.

À chaque amorçage du système, GRUB charge le fichier de menu depuis le système de fichiers. C'est pourquoi il est inutile de réinstaller GRUB après chaque modification de ce fichier. Utilisez le chargeur d'amorçage YaST pour modifier la configuration de GRUB, comme le décrit la Section 29.4, « Configuration du chargeur d'amorçage à l'aide de YaST » (p. 484).

Le fichier de menu contient des commandes. Leur syntaxe est très simple. Chaque ligne contient une commande suivie de paramètres facultatifs séparés par un espace, comme dans le shell. Pour des raisons historiques, certaines commandes autorisent l'ajout du signe = avant le premier paramètre. Les commentaires sont introduits par le signe dièse (#).

Pour identifier les éléments de menu dans l'aperçu du menu, attribuez un titre (`title`) à chaque entrée. Le texte (espaces compris) qui suit le mot-clé `title` apparaît dans le menu sous forme d'option à sélectionner. Toutes les commandes incluses avant l'argument de titre (`title`) suivant sont exécutées lors de la sélection de l'élément de menu correspondant.

Le cas le plus simple est la redirection vers des chargeurs d'amorçage d'autres systèmes d'exploitation. La commande est `chainloader` et l'argument est généralement le bloc d'amorçage d'une autre partition, exprimé dans la notation de blocs GRUB. Par exemple :

```
chainloader (hd0,3)+1
```

Les noms de périphérique dans GRUB sont présentés à la section intitulée « Conventions d'assignation de nom pour les disques durs et les partitions » (p. 476). L'exemple ci-dessus désigne le premier bloc de la quatrième partition du premier disque dur.

Utilisez la commande `kernel` pour spécifier une image de kernel. Le premier argument est le chemin de l'image de kernel dans une partition. Les autres arguments sont transmis au kernel sur la ligne de commande.

Si le kernel ne comporte pas les pilotes intégrés nécessaires pour accéder à la partition racine, vous devez spécifier le fichier `initrd` via une commande GRUB distincte, dont l'unique argument est le chemin du fichier `initrd`. Comme l'adresse de chargement du fichier `initrd` est écrite dans l'image de kernel chargée, la commande `initrd` doit suivre immédiatement la commande `kernel`.

La commande `root` simplifie la spécification des fichiers de kernel et du fichier initrd. Le seul argument de la commande `root` est un périphérique GRUB (ou une partition sur un périphérique GRUB). Ce périphérique est utilisé pour les chemins du fichier `initrd`, du fichier de kernel et de tout autre fichier pour lequel aucun périphérique n'est spécifié de manière explicite, jusqu'à la commande `root` suivante. Cette commande n'est pas utilisée dans le fichier `menu.lst` généré au cours de l'installation. Elle facilite simplement les modifications manuelles.

La commande `boot` est incluse de manière implicite à la fin de chaque entrée de menu ; par conséquent, il est inutile de l'ajouter dans le fichier de menu. Toutefois, si vous utilisez GRUB de manière interactive pour l'amorçage, vous devez ajouter la commande `boot` à la fin. Cette commande ne comporte aucun argument. Elle amorce simplement l'image de kernel chargée ou le chargeur chaîné indiqué.

Après avoir écrit toutes les entrées de menu, définissez l'une d'elles comme entrée par défaut (`default`). Sinon, le système utilise la première entrée (entrée `0`). Vous pouvez également préciser le timeout (en seconde) au bout duquel l'entrée par défaut doit être amorcée. Les entrées `timeout` et `default` précèdent généralement les entrées de menu. Un fichier d'exemple est fourni à la section intitulée « Exemple de fichier de menu » (p. 477).

Conventions d'assignation de nom pour les disques durs et les partitions

Les conventions d'assignation de nom utilisées par GRUB pour les disques durs et les partitions sont différentes de celles employées pour les périphériques Linux standard. Dans GRUB, la numérotation des partitions commence à zéro. Par conséquent, `(hd0,0)` désigne la première partition du premier disque dur. Sur un ordinateur de bureau standard doté d'un disque dur connecté en tant que maître primaire, le nom Linux du même périphérique est `/dev/hda1`.

Les quatre partitions primaires possibles portent les numéros de partition `0` à `3`. Les partitions logiques sont numérotées à partir de `4` :

```
(hd0,0)   première partition primaire du premier disque dur
(hd0,1)   deuxième partition primaire
(hd0,2)   troisième partition primaire
(hd0,3)   quatrième partition primaire (généralement, une partition étendue)
(hd0,4)   première partition logique
(hd0,5)   deuxième partition logique
```

GRUB ne fait pas de distinction entre les périphériques IDE, SCSI et RAID. Tous les disques durs reconnus par le BIOS (ou autres contrôleurs) sont numérotés en fonction de la séquence d'amorçage prédéfinie dans le BIOS.

GRUB n'est toutefois pas capable d'assigner correctement les noms de périphérique Linux aux noms de périphérique BIOS. Il génère cette assignation à l'aide d'un algorithme et l'enregistre dans le fichier `device.map`, que vous pouvez modifier si nécessaire. Pour obtenir des informations sur le fichier `device.map`, consultez la Section 29.3.2, « Fichier device.map » (p. 481).

Un chemin GRUB complet est composé d'un nom de périphérique entre parenthèses, avec le chemin du fichier tel qu'il est défini dans le système de fichiers de la partition indiquée. Le chemin commence par une barre oblique. Par exemple, le kernel amorçable sera spécifié comme suit sur un système avec un seul disque dur IDE où Linux est installé dans la première partition :

```
(hd0,0)/boot/vmlinuz
```

Exemple de fichier de menu

L'exemple suivant illustre la structure d'un fichier de menu GRUB. Dans notre exemple, l'installation comprend une partition d'amorçage Linux sous `/dev/hda5`, une partition racine sous `/dev/hda7` et une installation Windows sous `/dev/hda1`.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd

title windows
   chainloader(hd0,0)+1

title floppy
   chainloader(fd0)+1

title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

Le premier bloc définit la configuration de l'écran de démarrage :

gfxmenu (hd0,4)/message
L'image d'arrière-plan `message` se trouve dans `/dev/hda5`.

color white/blue black/light-gray
Modèle de couleurs : blanc (premier plan), bleu (arrière-plan), noir (sélection) et gris clair (arrière-plan de la sélection). Le modèle de couleurs ne s'applique pas à l'écran de démarrage, mais uniquement au menu GRUB personnalisable ; pour accéder à ce dernier, quittez l'écran de démarrage à l'aide de la touche Échap.

default 0
La première entrée de menu `title linux` est celle à amorcer par défaut.

timeout 8
Au bout de huit secondes sans saisie de la part de l'utilisateur, GRUB amorce automatiquement l'entrée par défaut. Pour désactiver l'amorçage automatique, supprimez la ligne `timeout`. Si vous entrez `timeout 0`, GRUB amorce immédiatement l'entrée par défaut.

Le second bloc (le plus volumineux) répertorie les différents systèmes d'exploitation amorçables. Les sections de chaque système d'exploitation commencent par `title`.

- La première entrée (`title linux`) contrôle l'amorçage de SUSE Linux. Le kernel (`vmlinuz`) se trouve dans la première partition logique (partition d'amorçage) du premier disque dur. Les paramètres de kernel, comme la partition racine et le mode VGA, sont ajoutés à la fin de cette ligne. La partition racine est spécifiée en utilisant la convention d'assignation de nom Linux (`/dev/hda7/`), car ces informations sont lues par le kernel et ne concernent pas GRUB. Le fichier `initrd` se trouve également dans la première partition logique du premier disque dur.

- La deuxième entrée concerne le chargement de Windows. Windows est amorcé à partir de la première partition du premier disque dur (`hd0,0`). La commande `chainloader +1` ordonne à GRUB de lire et d'exécuter le premier secteur de la partition indiquée.

- L'entrée suivante permet l'amorçage à partir d'une disquette, sans modification des paramètres du BIOS.

- L'option d'amorçage `failsafe` lance Linux avec un ensemble de paramètres de kernel permettant l'amorçage de Linux même sur des systèmes problématiques.

Vous pouvez modifier le fichier de menu chaque fois que cela s'avère nécessaire. Lors de l'amorçage suivant, GRUB utilise les paramètres modifiés. Pour modifier définitivement le fichier, utilisez YaST ou l'éditeur de votre choix. Vous pouvez aussi appliquer de manière interactive des modifications temporaires, via la fonction de modification de GRUB. (voir la section intitulée « Modification des entrées de menu au cours de la procédure d'amorçage » (p. 479)).

Modification des entrées de menu au cours de la procédure d'amorçage

Dans le menu graphique d'amorçage GRUB, sélectionnez le système d'exploitation à amorcer, à l'aide des touches fléchées. Si vous sélectionnez un système Linux, vous pouvez entrer des paramètres d'amorçage supplémentaires à l'invite d'amorçage. Pour modifier directement des entrées de menu précises, appuyez sur Échap pour quitter l'écran de démarrage, puis appuyez sur E. Les modifications effectuées ainsi ne s'appliquent qu'à la procédure d'amorçage actuelle et ne sont pas définitives.

IMPORTANT: Disposition du clavier au cours de la procédure d'amorçage

Seul le clavier américain est disponible lors de la procédure d'amorçage.

Une fois le mode de modification activé, utilisez les touches fléchées pour sélectionner l'entrée de menu dont vous souhaitez modifier la configuration. Pour pouvoir modifier la configuration, appuyez à nouveau sur la touche E. Procédez ainsi pour modifier les partitions ou les spécifications de chemin incorrectes, avant qu'elles aient une incidence néfaste sur le processus d'amorçage. Appuyez sur Entrée pour quitter le mode de modification et revenir au menu. Appuyez ensuite sur B pour amorcer cette entrée. Les autres actions possibles sont affichées dans le texte d'aide, au bas de la page.

Pour modifier définitivement des options d'amorçage et les transmettre au kernel, ouvrez le fichier `menu.lst` en tant qu'utilisateur `root`, puis ajoutez à la ligne existante les paramètres de kernel voulus, séparés par des espaces :

```
title linux
   kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
   initrd (hd0,0)/initrd
```

GRUB adopte automatiquement les nouveaux paramètres lors de l'amorçage suivant du système. Vous pouvez également apporter ces modifications à l'aide du module de

chargeur d'amorçage YaST. Ajoutez les nouveaux paramètres à la ligne existante, en les séparant par des espaces.

Utilisation de caractères joker pour sélectionner le kernel d'amorçage

Vous devez, en particulier lorsque vous développez ou utilisez des kernels personnalisés, modifier les entrées du fichier `menu.lst` ou la ligne de commande, afin de refléter les noms du fichier initrd et du fichier de kernel actuels. Pour simplifier cette procédure, utilisez des *caractères joker* pour mettre à jour dynamiquement la liste de kernels de GRUB. Toutes les images de kernel qui répondent à un modèle particulier sont automatiquement ajoutées à la liste des images amorçables. Aucun support technique n'est disponible pour cette fonctionnalité.

Pour activer l'option de caractère joker, saisissez une entrée de menu supplémentaire dans `menu.lst`. Pour être utilisées, toutes les images de kernel et de fichier initrd doivent porter un nom de base commun et un identificateur correspondant au kernel et au fichier initrd associé. Prenons, par exemple, la configuration suivante :

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

Dans ce cas, vous pouvez ajouter les deux images d'amorçage dans une même configuration GRUB. Pour obtenir les entrées de menu `linux-default` et `linux-test`, vous avez besoin de l'entrée suivante dans le fichier `menu.lst` :

```
title linux-*
    wildcard (hd0,4)/vmlinuz-*
    kernel (hd0,4)/vmlinuz-* root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd-*
```

Dans cet exemple, GRUB recherche dans la partition (hd0,4) les entrées qui correspondent au caractère joker. Ces entrées servent à générer de nouvelles entrées de menu GRUB. Dans l'exemple ci-dessus, GRUB se comporte comme si les entrées suivantes existaient dans le fichier `menu.lst` :

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
```

```
kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
initrd (hd0,4)/initrd-test
```

Cette configuration peut poser des problèmes si les noms de fichier ne sont pas cohérents ou si l'un des fichiers développés, comme une image initrd, est manquant.

29.3.2 Fichier device.map

Le fichier `device.map` assigne des noms de périphérique GRUB à des noms de périphérique Linux. Dans un système mixte comprenant à la fois des disques durs IDE et SCSI, GRUB doit tenter de déterminer la séquence d'amorçage à l'aide d'une procédure spéciale, car il n'a pas accès aux informations du BIOS concernant cette séquence. GRUB enregistre le résultat de cette analyse dans le fichier `/boot/grub/device.map`. Dans le cas d'un système où la séquence d'amorçage du BIOS est paramétrée sur « IDE avant SCSI », le fichier `device.map` peut apparaître sous la forme suivante :

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

Étant donné que l'ordre « IDE, SCSI, puis autres disques durs » dépend de divers facteurs et que Linux est incapable d'identifier l'assignation effectuée, vous pouvez définir manuellement la séquence dans le fichier `device.map`. Si vous rencontrez des problèmes lors de l'amorçage, vérifiez que la séquence figurant dans ce fichier correspond à celle du BIOS et, si tel n'est pas le cas, utilisez le shell GRUB (décrit à la Section 29.3.4, « Shell GRUB » (p. 482)) pour modifier temporairement la séquence. Une fois le système Linux amorcé, vous pouvez modifier définitivement le fichier `device.map` à l'aide du module de chargeur d'amorçage YaST ou de l'éditeur de votre choix.

Après avoir modifié manuellement le fichier `device.map`, exécutez la commande suivante pour réinstaller GRUB. Cette commande provoque le rechargement du fichier `device.map` et l'exécution des commandes répertoriées dans `grub.conf` :

```
grub --batch < /etc/grub.conf
```

29.3.3 Fichier /etc/grub.conf

Un troisième fichier de configuration GRUB important vient s'ajouter à `menu.lst` et `device.map` : `/etc/grub.conf`. Ce fichier contient les paramètres et options dont la commande `grub` a besoin pour installer correctement le chargeur d'amorçage.

```
root (hd0,4)
   install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
   quit
```

Signification de chaque entrée :

root (hd0,4)
: Cette commande demande à GRUB d'appliquer les commandes suivantes à la première partition logique du premier disque dur (emplacement des fichiers d'amorçage).

install `parameter`
: Vous devez exécuter la commande `grub` avec le paramètre `install`. Le niveau `stage1` du chargeur d'amorçage doit être installé dans le MBR (Master Boot Record - secteur d'amorçage principal) du premier disque dur (`/grub/stage1 d (hd0)`). Le niveau `stage2` doit être chargé vers l'adresse mémoire 0x8000 (`/grub/stage2 0x8000`). La dernière entrée (`(hd0,4)/grub/menu.lst`) indique à GRUB où rechercher le fichier de menu.

29.3.4 Shell GRUB

GRUB est en fait disponible en deux versions : en tant que chargeur d'amorçage et en tant que programme Linux standard dans `/usr/sbin/grub`. Ce programme est appelé *shell GRUB*. La fonctionnalité qui permet d'installer GRUB en tant que chargeur d'amorçage sur un disque dur ou une disquette est intégrée à GRUB, et inclut les commandes `install` et `setup`. Elle est disponible dans le shell GRUB une fois Linux chargé.

Vous pouvez également accéder aux commandes `setup` et `install` au cours de la procédure d'amorçage, avant le démarrage de Linux. Le dépannage d'un système défectueux qui ne peut plus être amorcé s'en trouve facilité ; en effet, vous pouvez résoudre le problème posé par le fichier de configuration du chargeur d'amorçage en entrant les paramètres manuellement. La saisie manuelle des paramètres au cours de la procédure d'amorçage s'avère également utile pour tester de nouveaux paramètres sans risquer de détériorer le système natif. Il vous suffit d'entrer le fichier de configuration de test en y incluant une syntaxe semblable à celle du fichier `menu.lst`. Testez ensuite la fonctionnalité de cette entrée sans modifier le fichier de configuration existant. Par exemple, pour tester un nouveau kernel, entrez la commande `kernel`, suivie du chemin du nouveau kernel. Si la procédure d'amorçage échoue, vous pouvez utiliser le fichier `menu.lst` intact pour effectuer l'amorçage suivant. De même, il est possible d'amorcer

un système même si le fichier menu.lst est défectueux, en entrant les paramètres corrigés dans l'interface de ligne de commande. Dans le système en cours d'exécution, les paramètres corrects peuvent être saisis dans le fichier menu.lst afin que ce système soit amorçable en permanence.

L'assignation de périphériques GRUB à des noms de périphérique Linux n'est possible que lorsque le shell GRUB est exécuté en tant que programme Linux (en entrant la commande grub de la manière indiquée à la Section 29.3.2, « Fichier device.map » (p. 481)). Pour ce faire, le programme lit le fichier device.map. Pour plus d'informations, consultez Section 29.3.2, « Fichier device.map » (p. 481).

29.3.5 Définition d'un mot de passe d'amorçage

Même avant l'amorçage du système d'exploitation, GRUB permet d'accéder à des systèmes de fichiers. Les utilisateurs sans autorisation racine (root) peuvent ainsi accéder à des fichiers de votre système Linux, auxquels ils n'ont plus accès une fois le système amorcé. Pour bloquer ce type d'accès ou empêcher les utilisateurs d'amorcer certains systèmes d'exploitation, définissez un mot de passe d'amorçage.

IMPORTANT: Mot de passe d'amorçage et écran de démarrage

Si vous utilisez un mot de passe d'amorçage pour GRUB, l'écran de démarrage habituel n'apparaît pas.

En tant qu'utilisateur root, définissez le mot de passe d'amorçage de la manière suivante :

1. À l'invite « root », entrez la commande grub.

2. Codez le mot de passe dans le shell GRUB :

```
grub> md5crypt
     Mot de passe : ****
     Version codée : $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. Collez la chaîne codée dans la section « global » du fichier menu.lst :

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
```

```
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Les commandes GRUB ne peuvent désormais être exécutées qu'à l'invite d'amorçage, après avoir appuyé sur P et saisi le mot de passe. Cependant, les utilisateurs peuvent toujours amorcer tous les systèmes d'exploitation à partir du menu d'amorçage.

4 Pour empêcher les utilisateurs d'amorcer un ou plusieurs systèmes d'exploitation à partir du menu d'amorçage, ajoutez l'entrée `lock` à chaque section du fichier `menu.lst`, afin que l'amorçage ne soit possible qu'après saisie d'un mot de passe. Par exemple :

```
title linux
kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
initrd (hd0,4)/initrd
lock
```

Si vous réamorcez le système et sélectionnez l'entrée Linux dans le menu d'amorçage, le message d'erreur suivant apparaît :

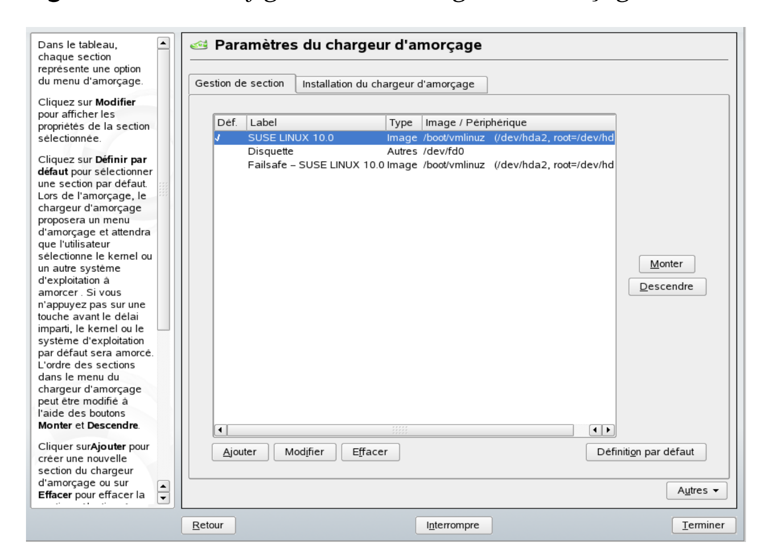
```
Error 32: Must be authenticated  (vous devez vous authentifier)
```

Appuyez sur Entrée pour entrer dans le menu. Appuyez ensuite sur P pour obtenir une invite de saisie de mot de passe. Une fois que vous avez saisi le mot de passe et appuyé sur Entrée, le système d'exploitation sélectionné (Linux, ici) doit s'amorcer.

29.4 Configuration du chargeur d'amorçage à l'aide de YaST

Le moyen le plus simple pour configurer le chargeur d'amorçage sur le système SUSE Linux consiste à utiliser le module YaST. Dans le centre de contrôle YaST, sélectionnez *Système → Configuration du chargeur d'amorçage*. La configuration actuelle du chargeur d'amorçage de votre système apparaît ; vous pouvez alors effectuer les modifications souhaitées. (voir Figure 29.1, « Configuration du chargeur d'amorçage à l'aide de YaST » (p. 485)).

Figure 29.1 Configuration du chargeur d'amorçage à l'aide de YaST



La fenêtre principale comporte deux onglets :

Gestion de section

Dans cet onglet, vous pouvez modifier et supprimer les sections du chargeur d'amorçage des différents systèmes d'exploitation. Pour ajouter une option, cliquez sur *Ajouter*. Pour modifier la valeur d'une option existante, sélectionnez l'option souhaitée, puis cliquez sur *Modifier*. Si l'une des options existantes ne présente aucune utilité pour vous, sélectionnez-la, puis cliquez sur *Supprimer*. Pour vous familiariser avec les options du chargeur d'amorçage, reportez-vous d'abord à la Section 29.3, « Amorçage à l'aide de GRUB » (p. 473).

Installation du chargeur d'amorçage

Utilisez cet onglet pour afficher ou modifier les paramètres liés au type, à l'emplacement ou à d'autres paramètres du chargeur d'amorçage.

29.4.1 Type de chargeur d'amorçage

Définissez le type de chargeur d'amorçage dans l'onglet *Installation du chargeur d'amorçage*. Dans SUSE Linux, le chargeur d'amorçage par défaut est GRUB. Pour utiliser LILO, procédez comme suit :

Procédure 29.2 *Modification du type du chargeur d'amorçage*

1. Accédez à l'onglet *Installation du chargeur d'amorçage*.

2. Dans le volet *Type*, cliquez sur le menu *Chargeur d'amorçage*, puis sélectionnez *LILO*.

3. Choisissez l'une des actions suivantes dans le menu contextuel :

   Proposer une nouvelle configuration
   YaST propose une nouvelle configuration.

   Convertir la configuration actuelle
   YaST convertit la configuration actuelle. Lors de la conversion de la configuration, vous risquez de perdre certains paramètres.

   Commencer une nouvelle configuration à zéro
   Cette option permet de créer une configuration personnalisée. Elle n'est pas disponible pendant l'installation de SUSE Linux.

   Lire la configuration enregistrée sur le disque
   Cette option vous permet de charger votre propre fichier `/etc/lilo.conf`. Elle n'est pas disponible pendant l'installation de SUSE Linux.

4. Cliquez sur *OK* pour enregistrer les modifications.

5. Dans la boîte de dialogue principale, cliquez sur *Terminer* pour que les modifications prennent effet.

Une fois la conversion effectuée, l'ancienne configuration GRUB est enregistrée sur le disque. Pour l'utiliser, il vous suffit de rétablir GRUB en tant que type du chargeur d'amorçage et de sélectionner l'option *Récupérer la configuration enregistrée avant la conversion* dans le menu contextuel. Cette opération n'est possible que sur un système installé.

REMARQUE: Chargeur d'amorçage personnalisé

Si vous souhaitez utiliser un autre chargeur d'amorçage que GRUB ou que LILO, cliquez sur l'option *Ne pas installer de chargeur d'amorçage*. Avant de choisir cette option, lisez attentivement la documentation de votre chargeur d'amorçage.

29.4.2 Emplacement du chargeur d'amorçage

Vous devrez peut-être modifier l'emplacement du chargeur d'amorçage. Le module YaST vous assiste dans cette tâche.

Procédure 29.3 *Modification de l'emplacement du chargeur d'amorçage*

1 Pour modifier l'emplacement du chargeur d'amorçage, cliquez sur l'onglet *Installation du chargeur d'amorçage*, puis sélectionnez l'une des options suivantes dans le menu *Emplacement du chargeur d'amorçage* :

Secteur maître d'amorçage de /dev/hdX
Amorçage principal d'un disque. Cette option est recommandée lorsque SUSE indique que le système peut être amorcé de cette manière. La lettre « X » correspond au disque dur, c'est-à-dire a, b, c ou d.

```
hda => ide0 master
     hdb => ide0 slave
     hdc => ide1 master
     hdd => ide1 slave
```

Secteur d'amorçage de la partition d'amorçage /dev/hdXY
Secteur d'amorçage de la partition d'amorçage `/boot`. Il s'agit de l'option par défaut lorsque plusieurs systèmes d'exploitation sont installés sur votre disque dur. La lettre « Y » représente la partition, soit 1, 2, 3, 4, 5, etc. Par conséquent, l'entrée peut avoir l'aspect suivant :

```
/dev/hda1
```

Secteur d'amorçage de la partition root /dev/hdXY
Secteur d'amorçage de la partition racine `/` (root). Cette option est également utilisée si plusieurs systèmes d'exploitation sont installés sur votre disque dur et que vous souhaitez continuer à utiliser votre ancien gestionnaire d'amorçage.

Autre
Cette option vous permet d'indiquer l'emplacement du chargeur d'amorçage.

2 Cliquez sur *Terminer* pour que les modifications prennent effet.

29.4.3 Système par défaut

Pour modifier le système par défaut, procédez comme suit :

Procédure 29.4 *Configuration du système par défaut*

1 Ouvrez l'onglet *Gestion de section*.

2 Sélectionnez dans la liste le système souhaité, ou cliquez sur *Monter* ou *Descendre*.

3 Cliquez sur *Défini par défaut*.

4 Cliquez sur *Terminer* pour que ces modifications prennent effet.

29.4.4 Timeout du chargeur d'amorçage

Le chargeur d'amorçage ne lance pas immédiatement le système par défaut. Pendant ce timeout, vous pouvez arrêter l'amorçage du système par défaut, et modifier le système à amorcer ou définir des paramètres de kernel. Pour augmenter ou réduire le timeout du chargeur d'amorçage, procédez comme suit :

Procédure 29.5 *Modification du timeout du chargeur d'amorçage*

1 Accédez à l'onglet *Installation du chargeur d'amorçage*.

2 Cliquez sur *Options du chargeur d'amorçage*.

3 Sélectionnez l'option *Mode d'amorçage*.

4 Dans *Mode d'amorçage*, modifiez la valeur de l'option *Lors de l'amorçage* ; pour ce faire, entrez une nouvelle valeur, cliquez sur le bouton fléché approprié ou utilisez les touches fléchées du clavier.

5 Cliquez sur *OK*.

6 Cliquez sur *Terminer* pour que les modifications prennent effet.

Vous pouvez choisir d'afficher le menu d'amorçage de manière permanente en sélectionnant l'option *Poursuivre l'amorçage après le délai*.

29.4.5 Paramètres de sécurité

Grâce à ce module YaST, vous pouvez également définir un mot de passe afin de protéger le chargeur d'amorçage. Vous obtenez ainsi un niveau de sécurité supplémentaire.

Procédure 29.6 *Définition d'un mot de passe pour le chargeur d'amorçage*

1. Accédez à l'onglet *Installation du chargeur d'amorçage*.

2. Cliquez sur *Options du chargeur d'amorçage*.

3. Dans *Paramètres du mot de passe*, cochez l'option *Protéger le chargeur d'amorçage par un mot de passe*, puis définissez le mot de passe.

4. Cliquez sur *OK*.

5. Cliquez sur *Terminer* pour que ces modifications prennent effet.

29.4.6 Ordre des disques

Si votre ordinateur dispose de plusieurs disques durs, vous pouvez indiquer la séquence d'amorçage des disques telle qu'elle est définie dans la configuration du BIOS de l'ordinateur (consultez la Section 29.3.2, « Fichier device.map » (p. 481)). Pour ce faire, procédez comme suit :

Procédure 29.7 *Définition de l'ordre des disques*

1. Accédez à l'onglet *Installation du chargeur d'amorçage*.

2. Cliquez sur *Détails d'installation du chargeur d'amorçage*.

3. Si plusieurs disques sont répertoriés, sélectionnez-en un, puis cliquez sur le bouton *Monter* ou *Descendre* afin de modifier l'ordre des disques affichés.

4 Cliquez sur *OK* pour enregistrer les modifications.

5 Cliquez sur *Terminer* pour que ces modifications prennent effet.

À l'aide de ce module, vous pouvez également remplacer le secteur d'amorçage principal par un code générique (ce qui amorce la partition active). Cliquez sur *Remplacer MBR par du code générique*, dans *Mise à jour de la zone système du disque*. Vous pouvez également cliquer sur *Activer la partition du chargeur d'amorçage* dans le même panneau pour activer la partition qui contient le chargeur d'amorçage. Cliquez sur *Terminer* pour que ces modifications prennent effet.

29.5 Désinstallation du chargeur d'amorçage Linux

Vous pouvez utiliser YaST pour désinstaller le chargeur d'amorçage Linux et restaurer l'état qu'avait le MBR avant l'installation de Linux. Au cours de l'installation, YaST crée automatiquement une copie de sauvegarde du MBR d'origine et restaure ce MBR sur demande, en écrasant GRUB.

Pour désinstaller GRUB, lancez le module de chargeur d'amorçage YaST (*Système → Configuration du chargeur d'amorçage*). Dans la première boîte de dialogue, sélectionnez *Remise à zéro → Restaurer le MBR du disque dur*, puis quittez la boîte de dialogue en cliquant sur *Terminer*. Dans le MBR, GRUB est écrasé par les données du MBR d'origine.

29.6 Créer des CD d'amorçage

Si vous rencontrez des problèmes pendant l'amorçage de votre système avec un gestionnaire d'amorçage ou si vous ne pouvez pas installer le chargeur d'amorçage dans le secteur maître d'amorçage (MBR) de votre disque dur ni sur une disquette, vous pouvez aussi créer un CD amorçable sur lequel sont gravés tous les fichiers nécessaires au démarrage de Linux. Votre ordinateur doit pour cela disposer d'un graveur de CD correctement installé.

Pour créer un CD-ROM d'amorçage avec GRUB, vous n'avez besoin que de `stage2_eltorito`, une forme spéciale de *stage2* et éventuellement d'un `menu.lst` optionnel

adapté à vos besoins. Les fichiers classiques stage1 et stage2 ne sont pas nécessaires.

Créez un répertoire dans lequel l'image ISO sera créée. par exemple avec les commandes cd /tmp et mkdir iso. Créez aussi un sous-répertoire pour GRUB à l'aide de mkdir -p iso/boot/grub. Copiez le fichier stage2_eltorito dans le répertoire grub :

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Copiez également le noyau (/boot/vmlinuz), initrd (/boot/initrd) et /boot/message dans iso/boot/ :

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

Pour que GRUB puisse trouver ces fichiers, copiez le fichier menu.lst dans iso/boot/grub et modifiez les chemins d'accès de façon à les faire pointer sur le lecteur de CD-ROM. Pour cela, remplacez dans les chemins d'accès le noms de périphérique des disques durs, de la forme (hd*), par le nom de périphérique du lecteur de CD-ROM, (cd) :

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
    initrd (cd)/boot/initrd
```

Enfin, créez une image ISO à l'aide de la commande suivante :

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Gravez le fichier obtenu grub.iso sur un CD avec le programme de votre choix.

29.7 Écran graphique SUSE

À partir de la version 7.2 de SUSE Linux, l'écran graphique apparaît sur la première console si l'option « vga=<valeur> » est utilisée en tant que paramètre de kernel. Lorsque vous réalisez une installation à l'aide de YaST, cette option est activée automatiquement,

en fonction de la résolution sélectionnée et de la carte graphique. Vous pouvez désactiver l'écran SUSE de trois manières :

Désactivation de l'écran SUSE lorsque c'est nécessaire
: Entrez la commande `echo 0 >/proc/splash` sur la ligne de commande pour désactiver l'écran graphique. Pour réactiver cette fonction, saisissez `echo 1 >/proc/splash`.

Désactivation par défaut de l'écran SUSE
: Ajoutez le paramètre de kernel `splash=0` à votre configuration de chargeur d'amorçage. Pour plus d'informations à ce sujet, consultez le Chapitre 29, *Chargeur d'amorçage* (p. 471). Toutefois, si vous préférez le mode texte, qui était celui par défaut dans les versions précédentes, entrez `vga=normal`.

Désactivation totale de l'écran SUSE
: Compilez un nouveau kernel et désactivez l'option *Use splash screen instead of boot logo* (Utiliser l'écran de démarrage au lieu du logo d'amorçage) dans la section *framebuffer support* (prise en charge du tampon de mémoire vidéo).

> **ASTUCE**
>
> La désactivation de la prise en charge du tampon de mémoire vidéo dans le kernel désactive aussi automatiquement l'écran de démarrage. Si vous exécutez votre système à l'aide d'un kernel personnalisé, SUSE ne peut pas assurer sa prise en charge.

29.8 Dépannage

Cette section répertorie certains des problèmes fréquemment rencontrés lors de l'amorçage avec GRUB et fournit une brève description des solutions possibles. Certains problèmes sont traités dans les articles de la base de données de support, à l'adresse suivante : `http://portal.suse.de/sdb/en/index.html`. Si le problème rencontré ne figure pas dans cette liste, utilisez la boîte de dialogue de recherche de la base de données de support, à l'adresse `https://portal.suse.com/PM/page/search.pm`, pour rechercher des mots-clés, comme *GRUB*, *amorçage* et *chargeur d'amorçage*.

GRUB et XFS

Le système de fichiers XFS ne laisse aucune place pour le niveau `stage1` dans le bloc d'amorçage de la partition. Par conséquent, n'indiquez pas de partition XFS comme emplacement du chargeur d'amorçage. Pour résoudre le problème, vous pouvez créer une partition d'amorçage distincte dans un format autre que XFS.

GRUB et JFS

Bien que techniquement réalisable, la combinaison de GRUB et d'un système de fichiers JFS est problématique. Dans cette situation, créez une partition d'amorçage distincte (`/boot`) et formatez-la en Ext2. Installez GRUB dans cette partition.

GRUB signale une erreur GRUB Geom (géométrie GRUB)

GRUB vérifie la géométrie des disques durs connectés lorsque le système est amorcé. Parfois, le BIOS renvoie des informations incohérentes et GRUB signale une erreur GRUB Geom (erreur de géométrie GRUB). Dans ce cas, utilisez LILO ou mettez à jour le BIOS. Pour obtenir des informations détaillées sur l'installation, la configuration et la maintenance de LILO, accédez à la base de données de support et entrez le mot-clé LILO.

GRUB renvoie également ce message d'erreur si Linux a été installé sur un disque dur supplémentaire qui n'a pas été enregistré auprès du BIOS. Le niveau *stage1* du chargeur d'amorçage est trouvé et chargé correctement, mais le niveau *stage2* est introuvable. Vous pouvez corriger ce problème en enregistrant le nouveau disque dur auprès du BIOS.

Un système comportant des disques durs IDE et SCSI ne s'amorce pas

Au cours de l'installation, YaST a peut-être mal déterminé la séquence d'amorçage des disques durs (et vous ne l'avez pas corrigée). Par exemple, GRUB peut considérer `/dev/hda` comme étant `hd0` et `/dev/sda` comme étant `hd1`, alors que, dans le BIOS, la séquence d'amorçage est inversée (SCSI *avant* IDE).

Dans ce cas, corrigez les disques durs au cours du processus d'amorçage, via la ligne de commande GRUB. Une fois le système amorcé, modifiez le fichier `device.map` afin d'appliquer définitivement la nouvelle assignation. Vérifiez ensuite les noms de périphérique GRUB dans les fichiers `/boot/grub/menu.lst` et `/boot/grub/device.map`, puis réinstallez le chargeur d'amorçage à l'aide de la commande suivante :

```
grub --batch < /etc/grub.conf
```

Amorçage de Windows à partir du deuxième disque dur

Certains systèmes d'exploitation, comme Windows, ne peuvent être amorcés qu'à partir du premier disque dur. Si ce type de système d'exploitation n'est pas installé sur le premier disque dur, vous pouvez effectuer une modification logique de l'entrée de menu correspondante.

```
...
title windows
map (hd0) (hd1)
map (hd1) (hd0)
chainloader(hd1,0)+1
...
```

Dans cet exemple, Windows est démarré à partir du deuxième disque dur. Pour ce faire, vous utilisez la commande `map` pour modifier l'ordre logique des disques durs. Ce changement n'a pas d'incidence sur la logique du fichier de menu GRUB. Par conséquent, le deuxième disque dur doit être associé à `chainloader`.

29.9 Pour plus d'informations

Pour plus d'informations sur GRUB, reportez-vous au site `http://www.gnu.org/software/grub/`. Si vous disposez de texinfo sur votre ordinateur, affichez les pages d'informations GRUB dans un shell, à l'aide de la commande `info grub`. Pour plus d'informations sur des problèmes particuliers, vous pouvez également rechercher le mot-clé « GRUB » dans la base de données de support, à l'adresse `http://portal.suse.de/sdb/en/index.html`.

Caractéristiques spécifiques à SUSE Linux

30

Ce chapitre débute par des informations à propos de divers paquetages logiciels, des consoles virtuelles et de la configuration du clavier. Il aborde ensuite divers composants logiciel tels que `bash`, `cron` et `logrotate`, qui ont été modifiés ou améliorés au cours des derniers cycles de développement. Même s'ils sont de taille ou d'importance mineure, les utilisateurs peuvent être amenés à modifier leur comportement par défaut car ces composants sont souvent étroitement liés au système. Le chapitre se termine par une section consacrée aux paramètres spécifiques aux langues et aux pays (I18N et L10N).

30.1 Informations à propos des paquetages logiciel spéciaux

Les programmes `bash`, `cron`, `logrotate`, `locate`, `ulimit` et `free`, ainsi que le fichier`resolv.conf`, sont très importants pour les administrateurs système et de nombreux utilisateurs. Les pages de manuel et d'informations constituent deux sources d'informations fort utiles à propos des commandes, mais ne sont pas toujours disponibles. GNU Emacs est un éditeur de texte populaire et largement configurable.

30.1.1 Paquetage bash et /etc/profile

Bash est le shell par défaut dans SUSE Linux. Lorsqu'il est utilisé en guise de shell de login, il lit plusieurs fichiers d'initialisation. Bash les traite dans leur ordre d'apparition au sein de la liste.

1. /etc/profile
2. ~/.profile
3. /etc/bash.bashrc
4. ~/.bashrc

Des réglages personnalisés peuvent être effectués dans ~/.profile ou dans ~/.bashrc. Pour assurer le bon traitement de ces fichiers, il est nécessaire de copier les réglages de base à partir de /etc/skel/.profile ou /etc/skel/.bashrc dans le répertoire privé de l'utilisateur. Il est conseillé de copier les paramètres de /etc/skel après toute mise à jour. Exécutez les commandes de shell suivantes pour éviter la perte de vos réglages personnels :

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Recopiez ensuite vos paramètres personnels à partir des fichiers *.old.

30.1.2 Paquetage cron

Si vous souhaitez exécuter des commandes régulièrement et automatiquement en arrière-plan à des heures prédéfinies, cron est traditionnellement l'outil à utiliser. cron est piloté à l'aide de tables horaires spécialement formatées. Certaines sont livrées avec le système, mais les utilisateurs peuvent créer leur propres tables si nécessaire.

Les tables cron se situent dans /var/spool/cron/tabs. /etc/crontab sert de table cron à l'échelle du système. Entrez le nom de l'utilisateur qui doit exécuter la commande directement après l'horaire. root est saisi dans Exemple 30.1, « Entrée dans /etc/crontab » (p. 496). Les tables spécifiques, stockées dans /etc/cron.d, ont le même format. Consultez la page de manuel cron (man cron).

***Exemple 30.1** Entrée dans /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Vous ne pouvez pas éditer /etc/crontab en appelant la commande crontab -e. Le fichier doit être directement chargé dans un éditeur, modifié puis enregistré.

Un certain nombre de paquetages installent des scripts de shell dans les répertoires /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly et /etc/cron.monthly, dont les instructions sont contrôlées par /usr/lib/cron/run-crons. /usr/lib/cron/run-crons est exécuté toutes les 15 minutes depuis la table principale (/etc/crontab). Ceci garantit que les processus qui risqueraient d'être oubliés sont exécutés à l'heure prévue.

Pour exécuter des scripts de maintenance périodique selon un rythme horaire, quotidien ou autre à l'heure de votre choix, supprimez régulièrement les fichiers d'horodatage à l'aide d'entrées dans /etc/crontab (voir Exemple 30.2, « /etc/crontab : Suppression des fichiers d'horodatage » (p. 497), qui supprime le script horaire avant chaque heure pleine, le script quotidien une fois par jour à 2h14, etc.).

Exemple 30.2 * /etc/crontab : Suppression des fichiers d'horodatage*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Les tâches quotidiennes de maintenance système ont été réparties dans divers scripts pour des raisons de clarté. Elles sont contenues dans le paquetage aaa_base. /etc/cron.daily contient, par exemple, les composants suse.de-backup-rpmdb, suse.de-clean-tmp ou suse.de-cron-local.

30.1.3 Fichiers journaux : paquetage logrotate

Parallèlement au kernel, toute une série de services système (*démons*) enregistrent régulièrement l'état du système ainsi que des événements spécifiques dans des fichiers journaux. Ceci permet à l'administrateur de vérifier régulièrement l'état du système à un moment donné, de déceler les erreurs ou les dysfonctionnements et de les réparer avec beaucoup de précision. Ces fichiers journaux sont normalement stockés dans /var/log conformément au FHS et s'allongent de jour en jour. Le paquetage logrotate permet de contrôler la croissance de ces fichiers.

Configuration

Configurez logrotate avec le fichier /etc/logrotate.conf. La spécification include configure notamment les fichiers supplémentaires à lire. SUSE Linux garantit que les programmes qui génèrent des fichiers journaux installent leurs fichiers de configuration individuels dans /etc/logrotate.d. Ce type de programme accompagne par exemple les paquetages apache2 (/etc/logrotate.d/apache2) et syslogd (/etc/logrotate.d/syslog).

Exemple 30.3 *Exemple pour /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate est contrôlé par l'intermédiaire de cron et exécuté quotidiennement par /etc/cron.daily/logrotate.

IMPORTANT

L'option create lit tous les réglages effectués par l'administrateur dans /etc/permissions*. Veillez à éviter tout conflit lié à des modifications personnelles.

30.1.4 Commande locate

locate, une commande permettant de rechercher rapidement des fichiers, ne fait pas partie des composants installés par défaut. Si vous désirez l'utiliser, installez le paquetage `find-locate`. Le processus updatedb est exécuté automatiquement toutes les nuits ou environ 15 minutes après le démarrage du système.

30.1.5 Commande ulimit

La commande `ulimit` (*limite d'utilisateurs*) permet de définir des limites pour l'utilisation des ressources système et de les afficher. `ulimit` est particulièrement utile pour limiter la mémoire disponible pour les applications. De cette façon, il est possible d'empêcher une application d'accaparer une trop grande quantité de mémoire, ce qui risquerait de compromettre la stabilité du système.

`ulimit` peut être assorti de diverses options. Pour limiter l'utilisation de la mémoire, utilisez les options répertoriées dans Tableau 30.1, « `ulimit` : paramétrage des ressources pour l'utilisateur » (p. 499).

Tableau 30.1 *ulimit : paramétrage des ressources pour l'utilisateur*

`-m`	Taille maximum de la mémoire physique
`-v`	Taille maximum de la mémoire virtuelle
`-s`	Taille maximum de la pile
`-c`	Taille maximum des fichiers core
`-a`	Affichage des limites fixées

Des paramètres valables pour l'ensemble du système peuvent être définis dans `/etc/profile`. Activez ici la création de fichiers core, requis par les programmeurs pour le *débogage*. Un utilisateur normal ne peut pas augmenter les valeurs spécifiées dans `/etc/profile` par l'administrateur système, mais peut définir des entrées spéciales dans `~/.bashrc`.

Exemple 30.4 *ulimit : réglages dans ~/.bashrc*

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Les quantités de mémoire doivent être spécifiées en Ko. Pour de plus amples informations, voir `man bash`.

IMPORTANT

Tous les shells ne prennent pas en charge les directives `ulimit`. PAM (par exemple, `pam_limits`) offre des possibilités de réglage complètes si vous dépendez de réglages limitatifs pour ces restrictions.

30.1.6 Commande free

La commande `free` peut sembler mal nommée de prime abord puisqu'elle indique la quantité de RAM qui est en cours d'utilisation. Cette information se trouve dans `/proc/meminfo`. De nos jours, les utilisateurs qui disposent d'un système d'exploitation moderne, tel que Linux, n'ont pas réellement à s'inquiéter au sujet de la mémoire. Le concept de *mémoire disponible* remonte à une époque antérieure à la gestion unifiée de la mémoire. Le slogan *la mémoire libre est de la mémoire inutile* sied bien à Linux. En effet, Linux a toujours fait de son mieux pour équilibrer les mémoires cache sans autoriser les zones de mémoire libres ou inutilisées.

À la base, le kernel ne dispose d'aucune information directe sur les applications ou données utilisateur. Au lieu de cela, il gère les applications et données de l'utilisateur dans un *cache de page*. Si la mémoire vient à manquer, une partie de son contenu est écrit dans la partition ou le fichier d'échange, où elle reste accessible à l'aide de la commande `mmap` (voir `man mmap`).

Le kernel comporte également d'autres caches, tels que le *cache de slab*, où sont stockés les caches utilisés pour l'accès réseau. Ceci peut expliquer les différences entre les compteurs dans `/proc/meminfo`. La plupart, mais pas tous, sont accessibles via `/proc/slabinfo`.

30.1.7 Fichier /etc/resolv.conf

La résolution des noms de domaine est gérée par l'intermédiaire du fichier `/etc/resolv.conf`. Voir Chapitre 40, *La résolution de noms* (p. 655).

Ce fichier est exclusivement mis à jour par le script `/sbin/modify_resolvconf`, aucun autre programme n'étant autorisé à modifier directement `/etc/resolv.conf`. L'application de cette règle est le seul moyen de garantir que la configuration réseau du système et les fichiers correspondants sont conservés dans un état cohérent.

30.1.8 Pages de manuel et d'informations

Pour certaines applications GNU (telles que tar), les pages de manuel ne sont plus entretenues. Pour ces commandes, utilisez l'option `--help` pour obtenir un aperçu rapide des pages d'informations, qui fournissent des renseignements plus approfondis. info est le système hypertexte de GNU. Une présentation de ce système est consultable en tapant `info info`. Les pages d'informations peuvent être visualisées avec Emacs en saisissant `emacs -f info` ou directement dans une console avec `info`. Vous pouvez également utiliser tkinfo, xinfo ou le système d'aide de SUSE pour afficher les pages d'informations.

30.1.9 Paramètres de GNU Emacs

GNU Emacs est un environnement de travail complexe. Les sections suivantes couvrent les fichiers de configuration traités au lancement de GNU Emacs. De plus amples informations sont disponibles à l'adresse `http://www.gnu.org/software/emacs/` .

Au démarrage, Emacs lit plusieurs fichiers qui contiennent les paramètres de l'utilisateur, de l'administrateur système et du distributeur pour la personnalisation ou la préconfiguration. Le fichier d'initialisation `~/.emacs` est installé dans les répertoires privés des utilisateurs respectifs sous `/etc/skel`. `.emacs`, à son tour, lit le fichier `/etc/skel/.gnu-emacs`. Pour personnaliser le programme, copiez `.gnu-emacs` dans le répertoire privé (avec `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) et effectuez les réglages souhaités à cet emplacement.

.gnu-emacs définit le fichier ~/.gnu-emacs-custom comme custom-file. Si les utilisateurs font des réglages à l'aide des options customize dans Emacs, ces paramètres sont enregistrés dans ~/.gnu-emacs-custom.

Avec SUSE Linux, le paquetage emacs installe le fichier site-start.el dans le répertoire /usr/share/emacs/site-lisp. Le fichier site-start.el est chargé avant le fichier d'initialisation ~/.emacs. site-start.el garantit, entre autres, que les fichiers de configuration spéciaux distribués avec des paquetages complémentaires d'Emacs, tel que psgml, sont chargés automatiquement. Les fichiers de configuration de ce type sont également situés dans /usr/share/emacs/site-lisp et commencent toujours par suse-start-. L'administrateur système local peut spécifier des paramètres pour l'ensemble du système dans default.el.

De plus amples informations à propos de ces fichiers sont disponibles dans le fichier d'info Emacs sous *Init File* : info:/emacs/InitFile. Des informations sur la manière de désactiver le chargement de ces fichiers (si nécessaire) sont fournies au même endroit.

Les composants d'Emacs sont répartis dans plusieurs paquetages :

- Le paquetage de base emacs.
- emacs-x11 (généralement installé) : le programme *avec* support X11.
- emacs-nox : le programme *sans* support X11.
- emacs-info : documentation en ligne au format info.
- emacs-el : fichiers de bibliothèque non compilés en Emacs Lisp. Ceux-ci ne sont pas requis pour l'exécution.
- De nombreux paquetages complémentaires peuvent être installés si nécessaire : emacs-auctex (pour LaTeX), psgml (pour SGML et XML), gnuserv (pour le fonctionnement client et serveur) et bien d'autres.

30.2 Consoles virtuelles

Linux est un système multiutilisateur et multitâche. Les avantages de ces caractéristiques sont appréciables même sur un PC autonome. En mode texte, six consoles virtuelles

sont disponibles. Vous pouvez basculer entre elles à l'aide des touches Alt + F1 à Alt + F6. La septième console est réservée à X, et la dixième affiche les messages de kernel. Un nombre plus ou moins important de consoles peut être attribué en modifiant le fichier /etc/inittab.

Pour basculer vers une console à partir de X sans le fermer, utilisez Ctrl + Alt + F1 à Ctrl + Alt + F6. Pour revenir à X, appuyez sur Alt + F7.

30.3 Affectation des touches du clavier

Pour normaliser l'affectation des touches du clavier dans les programmes, des modifications ont été apportées aux fichiers suivants :

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Ces changements concernent uniquement les applications qui utilisent des entrées terminfo ou dont les fichiers de configuration sont directement modifiés (vi, less, etc.). Les applications qui ne sont pas livrées avec SUSE Linux doivent être adaptées à ces réglages par défaut.

Sous X, les touches composées (séquences de touches) sont accessible avec Ctrl + Maj (droit). Consultez également l'entrée correspondante dans /usr/X11R6/lib/X11/Xmodmap.

D'autres réglages sont possibles à l'aide de l'extension X Keyboard (XKB). Cette extension est également utilisée par les environnements de bureau GNOME (gswitchit) et KDE (kxkb).

ASTUCE: Pour plus d'informations

Des information sur XKB sont disponibles dans /etc/X11/xkb/README et dans les documents qui y sont répertoriés.

Des informations détaillés sur la saisie en chinois, japonais et coréen (CJK) sont disponibles sur le site de Mike Fabian : http://www.suse.de/~mfabian/suse-cjk/input.html.

30.4 Paramètres spécifiques aux langues et aux pays

SUSE Linux est très largement internationalisé et peut être modifié de façon très souple en fonction des besoins locaux. En d'autres termes, l'internationalisation (*I18N*) permet des localisations (*L10N*) spécifiques. Les abréviations I18N et L10N sont formées des première et dernière lettre du mot abrégé, avec le nombre de lettres omises entre les deux.

Les réglages sont effectués à l'aide de variables LC_ définies dans le fichier /etc/sysconfig/language. Cela ne concerne pas seulement la *prise en charge de la langue maternelle*, mais aussi les catégories *messages* (langue), *jeu de caractères*, *ordre de tri*, *date et heure*, *nombres* et *monnaie*. Chacune de ces catégories peut être définie directement avec sa propre variable ou indirectement avec une variable maître dans le fichier language (voir la page de manuel locale).

RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY
Ces variables, qui sont transmises au shell sans le préfixe RC_, représentent les catégories répertoriées. Les profils de shell concernés sont répertoriés ci-dessous. Le paramètre en cours peut être affiché avec la commande locale.

RC_LC_ALL
Si elle est définie, cette variable remplace les valeurs des variables mentionnées précédemment.

RC_LANG
Si aucune des variables précédentes n'est définie, celle-ci est utilisée comme solution de secours. Par défaut, SUSE Linux définit uniquement `RC_LANG`. Ainsi, les utilisateurs peuvent saisir plus facilement leurs propres valeurs.

ROOT_USES_LANG
Variable `yes` ou `no`. Si elle est réglée sur `no`, `root` travaille toujours dans l'environnement POSIX.

Les autres variables peuvent être définies via l'éditeur sysconfig de YaST (voir Section 28.3.1, « Modification de la configuration système à l'aide de l'éditeur sysconfig de YaST » (p. 467)). Leur valeur contient le code de la langue, celui du pays, le codage et le modificateur. Les composants individuels sont séparés par des caractères spéciaux :

```
LANG=<langue>[[_<PAYS>].<codage>[@<modificateur>]]
```

30.4.1 Quelques exemples

Il est conseillé de toujours définir les codes de langue et de pays ensemble. Les paramètres de langue sont conformes à la norme ISO 639, disponible aux adresses `http://www.evertype.com/standards/iso639/iso639-en.html` et `http://www.loc.gov/standards/iso639-2/`. Les codes de pays sont conformes à la norme ISO 3166, disponible à l'adresse `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`.

Il ne serait pas logique de définir des valeurs pour lesquelles vous n'avez pas de fichiers de description utilisables dans `/usr/lib/locale`. Il est possible de créer des fichiers de description à partir des fichiers de `/usr/share/i18n`, à l'aide de la commande `localedef`. Les fichiers de description font partie du paquetage `glibc-i18ndata`. Un fichier de description pour `en_US.UTF-8` (anglais américain) peut être créé comme suit :

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

LANG=en_US.UTF-8
Ceci est le réglage par défaut si vous avez sélectionné l'anglais américain au cours de l'installation. Si vous avez sélectionné une autre langue, celle-ci est activée avec le codage de caractères UTF-8.

LANG=fr_FR.ISO-8859-1
: Ce paramètre règle la langue sur l'anglais, le pays sur États-Unis et le jeu de caractères sur `ISO-8859-1`. Ce jeu de caractères ne comprend pas le symbole de l'Euro, mais peut être utile pour les programmes qui ne sont pas encore compatibles avec `UTF-8`. La chaîne qui définit le jeu de caractères (ici, `ISO-8859-1`) est utilisée par des programmes comme Emacs.

LANG=en_IE@euro
: L'exemple ci-dessus inclut explicitement le signe Euro dans le paramètre de langue. En principe, ce réglage est obsolète car UTF-8 couvre également le signe Euro. Il n'est utile que pour les applications qui ne supportent pas UTF-8, mais ISO-8859-15.

SuSEconfig lit les variables dans `/etc/sysconfig/language` et écrit les modifications requises dans `/etc/SuSEconfig/profile` et `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` est lu ou *émis* par `/etc/profile`. `/etc/SuSEconfig/csh.cshrc` est émis par `/etc/csh.cshrc`. Ces opérations rendent les paramètres disponibles dans l'ensemble du système.

Les utilisateurs peuvent remplacer les paramètres par défaut du système en modifiant leur fichier `~/.bashrc`. Par exemple, si vous ne souhaitez pas utiliser le réglage système global `en_US` pour les messages des programmes, ajoutez `LC_MESSAGES=es_ES` pour afficher les messages en espagnol par exemple.

30.4.2 Paramètres de prise en charge des langues

En règle générale, les fichiers de la catégorie *messages* sont uniquement stockés dans le répertoire de la langue correspondante (par exemple `en`) pour avoir une solution de secours. Si vous réglez `LANG` sur `en_US` et qu'il n'existe pas de fichier de messages dans `/usr/share/locale/en_US/LC_MESSAGES`, le système utilise `/usr/share/locale/en/LC_MESSAGES`.

Une chaîne de repli peut également être définie, par exemple du breton au français ou du galicien à l'espagnol, puis au portugais :

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Le cas échéant, il est possible d'utiliser les variantes de norvégien Nynorsk et Bokmål (avec une possibilité de repli sur `no`) :

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

ou

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Notez qu'en norvégien, `LC_TIME` est aussi traité différemment.

Un problème peut survenir si un séparateur utilisé pour délimiter des groupes de chiffres est mal reconnu. C'est le cas si `LANG` est réglé sur un code composé de seulement deux lettres (par exemple, `de`), tandis que le fichier de définition utilisé par glibc se situe dans un chemin du type `/usr/share/lib/de_DE/LC_NUMERIC`. Dans ce cas, il faut régler `LC_NUMERIC` sur `de_DE` pour rendre la définition de séparateur visible par le système.

30.4.3 Pour plus d'informations

- *The GNU C Library Reference Manual*, chapitre « Locales and Internationalization ». Inclus dans `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, actuellement à l'adresse `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto*, de Bruno Haible : `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

Fonctionnement de l'imprimante 31

CUPS est le système d'impression standard de SUSE Linux. CUPS est très orienté utilisateur. Généralement, il est compatible avec LPRng ou peut le devenir assez facilement. LPRng est inclut dans SUSE Linux uniquement pour des raisons de compatibilité.

Les imprimantes se distinguent par leur interface (USB ou réseau) et par leur langage d'impression. Lors de l'achat d'une imprimante, assurez-vous que son interface est prise en charge par le matériel et qu'elle utilise un langage d'impression compatible. Les imprimantes peuvent être divisées en trois classes de langages d'impression :

Imprimantes PostScript
: PostScript est le langage d'impression dans lequel la plupart des travaux sous Linux (et Unix) sont générés et traités par le système d'impression interne. Ce langage est déjà assez ancien mais très efficace. Si les documents PostScript peuvent être traités directement par l'imprimante, sans être convertis par d'autres opérations du système d'impression, le nombre de sources d'erreurs potentielles est réduit. Comme les imprimantes PostScript sont vendues avec des licences dont les coûts sont généralement élevés, elles sont généralement plus chères que les imprimantes sans interpréteur PostScript.

Imprimante standard (langages comme PCL et ESC/P)
: Même si ces langages d'impression sont plutôt anciens, ils évoluent toujours afin de s'adapter aux nouvelles fonctionnalités des imprimantes. Avec les langages d'impression qu'il reconnaît, le système d'impression peut convertir les travaux PostScript vers le langage d'impression concerné, à l'aide de Ghostscript. Cette phase de traitement est appelée « interprétation ». Les langages les plus célèbres sont PCL, le plus utilisé par les imprimantes HP et leurs clones, et ESC/P, utilisé

par les imprimantes Epson. Ces langages d'impression sont généralement pris en charge par Linux et génère un résultat satisfaisant. Toutefois, Linux risque de ne pas pouvoir exploiter certaines fonctions des imprimantes les plus récentes, si les développeurs de programmes Open Source sont encore en train de travailler sur ces fonctions. À part les pilotes `hpijs` développés par HP, il n'existe actuellement aucun fabricant d'imprimantes qui développe des pilotes pour Linux et les met à la disposition des distributeurs Linux sous licence Open Source. La plupart de ces imprimantes se situent le plus souvent dans une fourchette de prix moyenne.

Imprimantes propriétaires (généralement, des imprimantes GDI)

Généralement, il n'existe qu'un seul pilote Windows (ou seulement quelques-uns) pour les imprimantes propriétaires. Ces imprimantes ne prennent pas en charge les langages d'impression courants et les langages qu'elles utilisent peuvent changer lors de la commercialisation d'un nouveau modèle. Pour plus d'informations, consultez Section 31.7.1, « Imprimantes sans prise en charge d'un langage d'impression standard » (p. 527).

Avant d'acheter une nouvelle imprimante, consultez les sources suivantes pour vérifier le degré de prise en charge de l'imprimante choisie :

- `http://cdb.suse.de/` : base de données d'imprimantes SUSE Linux
- `http://www.linuxprinting.org/` : base de données d'imprimantes sur LinuxPrinting.org
- `http://www.cs.wisc.edu/~ghost/` : page Web de Ghostscript
- `/usr/share/doc/packages/ghostscript/catalog.devices` : liste des pilotes intégrés

Les bases de données en ligne affichent toujours l'état actuel de la prise en charge sous Linux. Cependant, il est évident qu'une distribution Linux ne peut intégrer que les pilotes disponibles au moment de sa création. Ainsi, une imprimante actuellement classée comme « parfaitement compatible » peut ne pas avoir eu cet état au moment de la sortie de la dernière version de SUSE Linux. Par conséquent, les bases de données n'indiquent pas forcément l'état correct, mais fournissent uniquement une approximation.

31.1 Workflow du système d'impression

L'utilisateur crée un travail d'impression. Le travail d'impression se compose des données à imprimer et des informations destinées au spouleur, comme le nom de l'imprimante et de la file d'attente d'impression ; il peut aussi contenir des informations destinées au filtre, comme des options propres à l'imprimante.

Chaque imprimante possède une file d'attente d'impression dédiée. Le spouleur maintient le travail d'impression en file d'attente, jusqu'à ce que l'imprimante choisie soit prête à recevoir les données. Lorsque l'imprimante est prête, le spouleur lui envoie les données via le filtre et l'interface dorsale.

Le filtre convertit les données que l'utilisateur souhaite imprimer (ASCII, PostScript, PDF, JPEG, etc.) en données propres à l'imprimante (PostScript, PCL, ESC/P, etc.). Les fonctionnalités de l'imprimante sont décrites dans les fichiers PPD. Un fichier PPD contient des options propres à l'imprimante, ainsi que les paramètres nécessaires à leur activation. Le système de filtre vérifie que les options sélectionnées par l'utilisateur sont bien activées.

Si vous utilisez une imprimante PostScript, le système de filtre convertit les données en informations PostScript propres à l'imprimante. Cela ne nécessite pas de pilote d'imprimante. Avec une imprimante non PostScript, le système de filtre utilise Ghostscript pour convertir les données en données propres à l'imprimante. Cela exige un pilote d'imprimante Ghostscript compatible avec votre imprimante. L'interface dorsale reçoit du filtre les données propres à l'imprimante et les transmet à cette dernière.

31.2 Méthodes et protocoles de connexion d'imprimantes

Il existe plusieurs manières de connecter une imprimante au système. La configuration du système d'impression CUPS ne distingue pas les imprimantes locales et de celles qui sont connectées au système via le réseau. Sous Linux, les imprimantes locales doivent être connectées conformément aux instructions du manuel du fabricant de l'imprimante. CUPS prend en charge les connexions série, USB, parallèles et SCSI. Pour plus d'informations sur la connexion de l'imprimante, lisez l'article *CUPS en*

quelques mots dans la base de données de support, à l'adresse http://portal.suse.com. Pour trouver l'article, entrez *cups* dans la boîte de dialogue de recherche.

AVERTISSEMENT: Connexion à la machine avec un câble

Lorsque vous connectez une imprimante à une machine, n'oubliez pas que seuls les périphériques USB peuvent être connectés et déconnectés quand les équipements fonctionnent. Pour toute autre connexion, vous devez d'abord éteindre le système.

31.3 Installation du logiciel

PPD (PostScript Printer Description - Description d'imprimante PostScript) est le langage informatique qui décrit les propriétés (comme la résolution) et les options (comme la disponibilité d'une unité d'impression recto-verso) d'une imprimante. Ces descriptions sont nécessaires pour l'utilisation de diverses options d'imprimante dans CUPS. Sans fichier PPD, les données seraient transmises à l'imprimante sous leur forme « brute », ce qui n'est généralement pas souhaitable. Au cours de l'installation de SUSE Linux, de nombreux fichiers PPD sont préinstallés pour permettre l'utilisation de toutes les imprimantes, même celles sans prise en charge de PostScript.

Pour configurer une imprimante PostScript, le meilleur moyen est d'obtenir le fichier PPD approprié. De nombreux fichiers PPD sont disponibles dans le paquetage `manufacturer-PPDs`, installé automatiquement lors d'une installation standard. Consultez la Section 31.6.3, « Fichiers PPD dans différents paquetages » (p. 524) et la Section 31.7.2, « Aucun fichier PPD approprié disponible pour une imprimante PostScript » (p. 528).

Vous pouvez également stocker de nouveaux fichiers PPD dans le répertoire `/usr/share/cups/model/` ou les ajouter au système d'impression, à l'aide de YaST (consultez la section intitulée « Configuration manuelle » (p. 514)). Ensuite, vous pouvez sélectionner ce fichier PPD au cours de l'installation.

Soyez prudent si un fabricant d'imprimante vous demande non seulement de modifier les fichiers de configuration mais également d'installer des paquetages logiciels complets. D'une part, ce type d'installation risque de vous faire perdre l'assistance technique fournie par SUSE Linux et, d'autre part, les commandes d'impression risquent de ne plus fonctionner de la même manière et vous risquez de ne plus pouvoir utiliser les

périphériques provenant d'autres fabricants. C'est pourquoi il est déconseillé d'installer un logiciel fourni par le fabricant.

31.4 Configuration de l'imprimante

Après avoir connecté l'imprimante à l'ordinateur et installé le logiciel, installez l'imprimante dans le système. Cette opération doit être effectuée à l'aide des outils fournis par SUSE Linux. Comme la sécurité est très importante pour SUSE Linux, les outils tiers posent souvent des problèmes, à cause des restrictions de sécurité, et apportent plus d'inconvénients que d'avantages. Pour plus d'informations sur le dépannage, consultez la Section 31.6.1, « Serveur CUPS et pare-feu » (p. 521) et la Section 31.6.2, « Modifications du service d'impression CUPS » (p. 522).

31.4.1 Imprimantes locales

Si, lorsque vous vous connectez, une imprimante locale non configurée est détectée, YaST démarre pour vous permettre de la configurer. Cette opération utilise les mêmes boîtes de dialogue dans la description suivante.

Pour configurer l'imprimante, sélectionnez *Matériel* → *Imprimante* dans le centre de contrôle YaST. La fenêtre principale de configuration des imprimantes s'ouvre et affiche la liste des périphériques détectés, dans sa partie supérieure. La partie inférieure de la fenêtre répertorie toutes les files d'attente configurées. Si votre imprimante n'a pas été détectée, configurez-la manuellement.

IMPORTANT

Si le menu *Imprimante* n'est pas disponible dans le centre de contrôle YaST, le paquetage `yast2-printer` n'est probablement pas installé. Pour résoudre ce problème, installez le paquetage `yast2-printer`, puis redémarrez YaST.

Configuration automatique

YaST est capable de configurer automatiquement l'imprimante si le port parallèle ou USB peut être configuré automatiquement, et si l'imprimante connectée peut être détectée. La base de données des imprimantes doit également contenir la chaîne d'ID

de l'imprimante, que YaST récupère lors de la détection automatique du nouveau matériel. Si l'ID de matériel diffère de la désignation du modèle, sélectionnez le modèle manuellement.

Pour vous assurer que tout fonctionne correctement, vous devez vérifier chaque configuration avec la fonction de test d'impression de YaST. La page de test fournit également des informations importantes sur la configuration testée.

Configuration manuelle

Si les caractéristiques de votre système ne permettent pas la configuration automatique ou si vous souhaitez personnaliser la configuration, configurez l'imprimante manuellement. Selon la réussite de la détection automatique et la quantité d'informations sur le modèle de l'imprimante figurant dans la base de données, YaST peut déterminer automatiquement les paramètres corrects ou, au moins, proposer une présélection rationnelle.

Les paramètres suivants doivent être configurés :

Connexion matérielle (port)

La configuration de la connexion matérielle dépend de la capacité de YaST à détecter l'imprimante au cours de la détection automatique du matériel. Si YaST a pu détecter le modèle d'imprimante automatiquement, vous pouvez considérer que la connexion de l'imprimante fonctionne au niveau matériel et qu'il est inutile d'en modifier les paramètres. Si YaST n'a pas pu détecter automatiquement le modèle d'imprimante, il peut y avoir un problème de connexion au niveau matériel. Dans ce cas, une intervention manuelle s'impose pour configurer la connexion.

Dans la boîte de dialogue *Configuration de l'imprimante*, cliquez sur *Configurer* pour démarrer le workflow de configuration manuelle. Ensuite, sélectionnez votre *type d'imprimante* (par exemple, `Imprimante USB`), puis cliquez sur *Suivant*, indiquez la *connexion d'imprimante* et sélectionnez le périphérique.

Nom de la file d'attente

Le nom de la file d'attente est utilisé lors de l'émission de commandes d'impression. Le nom doit être assez court, et ne contenir que des lettres minuscules et des chiffres. Entrez le *nom pour l'impression* dans la boîte de dialogue suivante (*Nom de la file d'impression*).

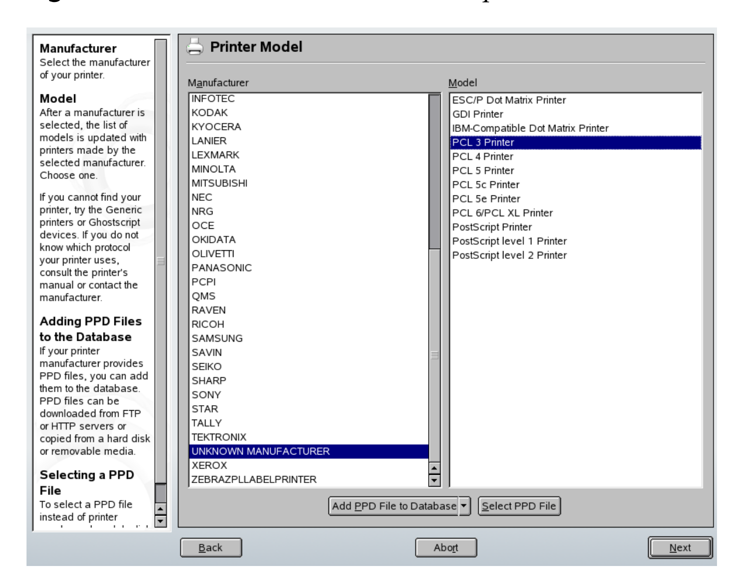
Modèle d'imprimante et fichier PPD

Tous les paramètres propres à l'imprimante, comme le pilote Ghostscript à utiliser et les paramètres de filtrage d'impression pour le pilote, sont stockés dans un fichier PPD (PostScript Printer Description - Description d'imprimante PostScript). Pour plus d'informations sur les fichiers PPD, consultez la Section 31.3, « Installation du logiciel » (p. 512).

Pour de nombreux modèles d'imprimante, plusieurs fichiers PPD sont disponibles, notamment lorsque plusieurs pilotes Ghostscript fonctionnent avec le modèle concerné. Lorsque vous sélectionnez un fabricant et un modèle dans la boîte de dialogue suivante (*Modèle d'imprimante*), YaST sélectionne le fichier PPD correspondant à l'imprimante. Si plusieurs fichiers PPD correspondent au modèle, YaST sélectionne l'un d'eux par défaut (normalement, celui qui porte la mention `recommandé`). Vous pouvez changer le fichier PPD choisi dans la boîte de dialogue suivante, avec l'option *Modifier*.

Pour les modèles non PostScript, toutes les données propres à l'imprimante sont générées par le pilote Ghostscript. C'est pourquoi la configuration du pilote est le seul facteur qui détermine réellement la qualité d'impression. Les impressions sont influencées à la fois par le type de pilote (fichier PPD) sélectionné et par les options spécifiées pour ce pilote. Si nécessaire, vous pouvez changer d'autres options (disponibles dans le fichier PPD) après avoir sélectionné l'option *Modifier*.

Figure 31.1 Sélection du modèle d'imprimante



Vérifiez toujours que vos réglages fonctionnent correctement, en imprimant une page de test. Si l'impression est illisible ou si plusieurs pages sont vides, par exemple, vous devez arrêter l'imprimante en commençant par retirer tout le papier, puis en arrêtant le test à partir de YaST.

Si la base de données des imprimantes ne contient pas le modèle de votre imprimante, vous pouvez ajouter un nouveau fichier PPD en sélectionnant *Ajout de fichiers PDD dans la base de données* ou utiliser un ensemble de fichiers PPD génériques pour que votre imprimante fonctionne avec l'un des langages d'impression standard. Pour cela, sélectionnez *FABRICANT INCONNU* comme fabricant de votre imprimante.

Paramètres avancés
Normalement, vous n'avez pas besoin de modifier ces paramètres.

31.4.2 Imprimantes réseau

Une imprimante réseau peut prendre en charge divers protocoles, dont certains simultanément. Même si la plupart des protocoles sont normalisés, certains fabricants étendent (modifient) le standard car ils testent des systèmes sur lesquels le standard n'est pas correctement implémenté ou parce qu'ils souhaitent fournir certaines fonctions qui ne

sont pas disponibles en standard. Les fabricants fournissent alors des pilotes pour un nombre restreint de systèmes d'exploitation, afin de corriger les problèmes liés à ces systèmes. Malheureusement, les pilotes Linux ne sont que rarement fournis. La situation actuelle est telle qu'il est impossible de considérer que tous les protocoles fonctionnent correctement sous Linux. Par conséquent, vous pouvez être amené à tester diverses options afin d'obtenir une configuration opérationnelle.

CUPS prend en charge les protocoles `socket`, `LPD`, `IPP` et `smb`. Vous trouverez ci-dessous des informations détaillées sur ces protocoles :

socket

Socket fait référence à une connexion dans laquelle les données sont envoyées à un socket Internet sans passer par l'étape de reconnaissance mutuelle préalable. Les numéros de port du socket couramment utilisés sont notamment `9100` ou `35`. Voici un exemple d'URI de périphérique : `socket://host-printer:9100/`.

LPD (Line Printer Daemon)

Le protocole LPD, déjà assez ancien, est décrit dans le document RFC 1179. Sous ce protocole, certaines données associées à un travail, comme l'ID de la file d'attente d'impression, sont envoyées avant les données à imprimer. Par conséquent, vous devez spécifier une file d'attente d'impression lorsque vous configurez le protocole LPD pour la transmission des données. Les implémentations des différents fabricants d'imprimante sont assez polyvalentes pour accepter n'importe quel nom de file d'attente d'impression. Si nécessaire, le manuel de l'imprimante vous indique le nom à utiliser. LPT, LPT1, LP1 (ou des noms similaires) sont souvent utilisés. Vous pouvez également configurer une file d'attente LPD sur un autre hôte Linux ou Unix du système CUPS. Le numéro de port d'un service LPD est `515`. Voici un exemple d'URI de périphérique : `lpd://host-printer/LPT1`.

IPP (Internet Printing Protocol)

IPP est un protocole assez récent (1999) qui repose sur le protocole HTTP. IPP permet de transmettre davantage de données de travail d'impression que les autres protocoles. CUPS utilise IPP pour la transmission des données internes. Il s'agit du meilleur protocole pour transférer des files d'attente entre deux serveurs CUPS. Vous devez spécifier le nom de la file d'attente d'impression pour configurer IPP correctement. Le numéro de port d'IPP est `631`. Voici des exemples d'URI de périphérique : `ipp://host-printer/ps` et `ipp://host-cupsserver/printers/ps`.

SMB (partage Windows)

CUPS prend également en charge l'impression sur des imprimantes connectées sur des partages Windows. Le protocole utilisé dans ce cas est SMB. SMB utilise les numéros de port `137`, `138` et `139`. Voici des exemples d'URI de périphérique : `smb://user:password@workgroup/server/printer`, `smb://user:password@host/printer` et `smb://server/printer`.

Le protocole pris en charge par l'imprimante doit être déterminé avant la configuration. Si le fabricant ne fournit pas les informations nécessaires, la commande `nmap`, qui figure dans le paquetage `nmap`, permet de déterminer le protocole. En effet, `nmap` recherche des ports ouverts sur un hôte. Par exemple :

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

Configuration de CUPS en réseau avec YaST

Les imprimantes réseau doivent être configurées avec YaST. YaST facilite la configuration et est mieux équipé pour gérer les restrictions de sécurité inhérentes à CUPS (consultez la Section 31.6.2, « Modifications du service d'impression CUPS » (p. 522)). Pour obtenir des instructions pour l'installation de CUPS en réseau, lisez l'article *CUPS en quelques mots* dans la base de données de support, à l'adresse `http://portal.suse.com`.

Choisissez *Autre (non détecté)* et cliquez sur *Configurer*. Sauf avis contraire de l'administrateur système, essayez l'option *Imprimer directement sur une imprimante en réseau* et poursuivez la configuration en fonction de vos besoins locaux.

Configuration à l'aide d'outils de ligne de commande

Vous pouvez également configurer CUPS à l'aide d'outils de ligne de commande, comme `lpadmin` et `lpoptions`. Vous devez disposer d'un URI (Uniform Resource Identifier - Identificateur uniforme de ressource) de périphérique qui se compose d'une interface dorsale, comme USB, et de paramètres comme `/dev/usb/lp0`. Par exemple, l'URI complet peut être `parallel:/dev/lp0` (imprimante connectée au premier port parallèle) ou `usb:/dev/usb/lp0` (première imprimante détectée connectée au port USB).

Avec la commande `lpadmin`, l'administrateur du serveur CUPS peut ajouter, supprimer et gérer les classes, ainsi que les files d'attente d'impression. Pour ajouter une file d'attente d'impression, utilisez la commande suivante :

```
lpadmin -p queue -v device-URI \
-P PPD-file -E
```

Ainsi, le périphérique (`-v`) sera disponible comme file d'attente *`queue`* (`-p`), en utilisant le fichier PPD spécifié (`-P`). Cela implique que vous devez connaître le fichier PPD et le nom du périphérique si vous souhaitez configurer l'imprimante manuellement.

N'utilisez pas `-E` comme première option. En effet, pour toutes les commandes CUPS, l'utilisation de l'option `-E` comme premier argument active l'utilisation d'une connexion codée. Pour activer l'imprimante, l'option `-E` doit être utilisée conformément à l'exemple suivant :

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

L'exemple suivant permet de configurer une imprimante réseau :

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Pour connaître les autres options de `lpadmin`, consultez la page de manuel `lpadmin(1).`

Au cours de l'installation du système, certaines options sont définies par défaut. Ces options peuvent être modifiées pour chaque travail d'impression (en fonction de l'outil d'impression utilisé). Vous pouvez également modifier ces options par défaut à l'aide de YaST. À l'aide des outils de ligne de commande, définissez les options par défaut de la manière suivante :

1 D'abord, répertoriez toutes les options :

```
lpoptions -p queue -l
```

Exemple :

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

L'option activée par défaut est mise en évidence par un astérisque (`*`).

2 Modifiez l'option avec `lpadmin` :

```
lpadmin -p queue -o Resolution=600dpi
```

3 Vérifiez le nouveau réglage :

```
lpoptions -p queue -l
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Lorsqu'un utilisateur normal exécute la commande `lpoptions`, les réglages sont enregistrés dans `~/.lpoptions`. Les réglages effectués par l'utilisateur `root` sont enregistrés dans `/etc/cups/lpoptions`.

31.5 Configuration des applications

Les applications comptent sur les files d'attente d'impression existantes, tout comme les outils de ligne de commande. Il est généralement inutile de reconfigurer l'imprimante pour une application particulière, car vous devriez pouvoir imprimer depuis des applications en utilisant les files d'attente existantes.

Pour imprimer depuis la ligne de commande, saisissez `lp -d` *`nom de file d'attente nom de fichier`*, en remplaçant *`nom de file d'attente`* et *`nom de fichier`* par les noms correspondants.

Certaines applications utilisent la commande `lp` pour imprimer. Dans ce cas, entrez la commande correcte dans la boîte de dialogue d'impression de l'application, sans spécifier de *`nom de fichier`*, par exemple, `lp -d` *`nom de file d'attente`*. Pour que cela fonctionne avec les programmes KDE, activez l'option d'*impression via un programme externe*. Sinon, vous ne pourrez pas saisir de commande d'impression.

Les outils comme xpp et le programme KDE kprinter offrent une interface graphique pour la sélection des files d'attente d'impression, et pour la configuration des options standard CUPS et des options spécifiques de l'imprimante accessibles via le fichier PPD. Vous pouvez utiliser kprinter comme interface standard d'impression des applications non-KDE en spécifiant `kprinter` ou `kprinter --stdin` comme commande d'impression dans les boîtes de dialogue d'impression de ces applications. C'est le comportement de l'application proprement dite qui détermine la commande à choisir. Si elle est correctement configurée, l'application devrait appeler la boîte de dialogue kprinter chaque fois qu'un travail d'impression est soumis ; ainsi, vous pouvez utiliser la boîte de dialogue pour sélectionner une file d'attente d'impression et d'autres options d'impression. Pour cela, la configuration d'impression propre à l'application ne doit pas entrer en conflit avec celle de kprinter et les options d'impression ne doivent être modifiées que par l'intermédiaire de kprinter, une fois ce programme activé.

31.6 Particularités de SUSE Linux

Quelques fonctionnalités de CUPS ont été adaptées pour SUSE Linux. Certains des principaux changements sont décrits ci-dessous.

31.6.1 Serveur CUPS et pare-feu

Il existe différentes manières de configurer CUPS comme client d'un serveur réseau.

1. Pour chaque file d'attente du serveur, vous pouvez configurer une file d'attente locale, par l'intermédiaire de laquelle vous envoyez tous les travaux d'impression au serveur réseau correspondant. Cette approche est généralement déconseillée car toutes les machines client doivent être reconfigurées dès que la configuration du serveur réseau est modifiée.

2. Les travaux d'impression peuvent également être transférés directement vers un seul serveur d'impression. Dans ce type de configuration, n'exécutez pas un démon CUPS local. La commande `lp` ou les appels de bibliothèque correspondants (ou tout autre programme) peuvent envoyer leurs travaux directement au serveur réseau. Cependant, cette configuration n'est pas adaptée à l'impression sur une imprimante locale.

3. Le démon CUPS peut écouter les paquets de diffusion IPP envoyés par d'autres serveurs réseau pour annoncer les files d'attente disponibles. Pour utiliser cette méthode, le port 631/UDP doit être ouvert et accepter les paquets entrants.

   C'est la meilleure configuration de CUPS pour imprimer via des serveurs CUPS distants. Toutefois, il existe un risque d'attaque par un pirate, s'il envoie des paquets de diffusion IPP mentionnant des files d'attentes et si le démon local accède à cette file d'attente contrefaite. Si le système affiche ensuite une file d'attente portant le même nom que qu'une autre file d'attente sur le serveur local, le propriétaire du travail peut croire qu'il envoie son travail vers un serveur local, alors qu'il l'envoie sur le serveur du pirate.

YaST peut trouver les serveurs CUPS en balayant tous les hôtes réseau pour vérifier s'ils offrent ce service et en écoutant les paquets de diffusion IPP. La deuxième méthode est utilisée lors de l'installation du système pour trouver les serveurs CUPS appropriés. Cela exige que le port 631/UDP soit ouvert et qu'il accepte les paquets entrants. L'ouverture d'un port à l'aide de la seconde méthode pour configurer l'accès à des files

d'attente distantes comporte un risque en matière de sécurité car un attaquant peut diffuser un serveur qui risque d'être accepté par les utilisateurs.

Le réglage par défaut du pare-feu affiché dans la boîte de dialogue de suggestion consiste à rejeter les diffusions IPP, quelle que soit l'interface. Ainsi, la deuxième méthode de détection des files d'attente et la troisième méthode d'accès aux files d'attente ne fonctionnent pas. Par conséquent, vous devez modifier la configuration du pare-feu en marquant l'une des interfaces comme `interne`, ce qui ouvre le port par défaut, ou en ouvrant explicitement le port d'une interface `externe`. Pour des raisons de sécurité, aucun port n'est ouvert par défaut.

La configuration de pare-feu proposée doit être modifiée, afin de permettre à CUPS de détecter les files d'attente distantes lors de l'installation et d'accéder à des serveurs distants à partir du système local au cours du fonctionnement normal. L'utilisateur peut également détecter les serveurs CUPS en balayant les hôtes du réseau local ou en configurant manuellement toutes les files d'attente. Cependant, pour les raisons déjà mentionnées au début de cette section, cette méthode est déconseillée.

31.6.2 Modifications du service d'impression CUPS

Ces modifications sont apparues dans SUSE Linux 9.1.

cupsd fonctionne avec le nom d'utilisateur lp

Au démarrage, `cupsd` passe de l'utilisateur `root` à l'utilisateur `lp`. Cela assure un niveau de sécurité beaucoup plus élevé, car le service d'impression CUPS ne fonctionne plus avec des droits illimités, mais uniquement avec les permissions nécessaires au service d'impression

Cependant, l'authentification (vérification du mot de passe) ne peut pas être effectuée via `/etc/shadow` car `lp` n'a pas accès à `/etc/shadow`. Vous devez utiliser à la place l'authentification propre à CUPS, via `/etc/cups/passwd.md5`. Pour ce faire, entrez le nom d'un administrateur CUPS membre du groupe d'administration CUPS `sys`, ainsi qu'un mot de passe CUPS, dans `/etc/cups/passwd.md5`. Pour ce faire, loguez-vous comme utilisateur `root` et entrez la commande suivante :

```
lppasswd -g sys -a CUPS-admin-name
```

Ce paramètre est également essentiel si vous souhaitez utiliser d'interface client Web d'administration (CUPS) ou l'outil d'administration d'imprimante (KDE).

Lorsque `cupsd` fonctionne avec le nom d'utilisateur `lp`, `/etc/printcap` ne peut pas être généré car `lp` n'est pas autorisé à créer des fichiers dans `/etc/`. Par conséquent, `cupsd` génère `/etc/cups/printcap`. Pour garantir que les applications qui ne peuvent lire les noms de file d'attente que depuis `/etc/printcap` continuent à fonctionner correctement, `/etc/printcap` est un lien symbolique qui pointe vers `/etc/cups/printcap`.

Lorsque `cupsd` s'exécute avec le nom d'utilisateur `lp`, le port `631` ne peut pas être ouvert. Par conséquent, `cupsd` ne peut pas être rechargé avec la commande `rccups reload`. Utilisez `rccups restart` à la place.

Fonctionnalité étendue pour `BrowseAllow` et `BrowseDeny`

Les autorisations d'accès définies pour `BrowseAllow` et `BrowseDeny` s'appliquent à tous les types de paquetages envoyés à `cupsd`. Les paramètres par défaut figurant dans le fichier `/etc/cups/cupsd.conf` sont les suivants :

```
BrowseAllow @LOCAL
BrowseDeny All
```

et

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

Ainsi, seuls les hôtes locaux (`LOCAL`) ont accès à la commande `cupsd` sur un serveur CUPS. Les hôtes `LOCAL` sont ceux dont les adresses IP appartiennent à une interface non-PPP (interfaces dont les indicateurs `IFF_POINTOPOINT` ne sont pas définis) et au même réseau que le serveur CUPS. Les paquets provenant de tous les autres hôtes sont immédiatement rejetés.

`cupsd` activé par défaut

Dans une installation standard, la commande `cupsd` est activée automatiquement, ce qui permet un accès confortable aux files d'attente des serveurs réseau CUPS sans autre opération manuelle. Les éléments indiqués à la section intitulée « cupsd fonctionne avec le nom d'utilisateur lp » (p. 522) et à la section intitulée « Fonctionnalité étendue pour `BrowseAllow` et `BrowseDeny` » (p. 523) sont des conditions préalables essentielles pour cette fonctionnalité ; en effet, si ces éléments ne sont pas appliqué, la sécurité est insuffisante pour une activation automatique de la commande `cupsd`.

31.6.3 Fichiers PPD dans différents paquetages

La configuration d'imprimante YaST configure les files d'attente de CUPS en utilisant uniquement les fichiers PPD installés dans `/usr/share/cups/model/` sur le système. Pour trouver les fichiers PPD adaptés au modèle de l'imprimante, YaST compare le fabricant et le modèle déterminé au cours de la détection du matériel avec les fabricants et modèles indiqués dans les fichiers PPD disponibles dans `/usr/share/cups/model/` sur le système. Pour cela, la configuration d'imprimante YaST génère une base de données à partir des informations relatives au fabricant et au modèle, extraites des fichiers PPD. Lorsque vous sélectionnez une imprimante dans la liste des fabricants et modèles, vous recevez les fichiers PPD correspondants.

Comme la configuration utilise uniquement des fichiers PPD et aucune autre source d'informations, vous avez l'avantage de pouvoir modifier librement les fichiers PPD dans `/usr/share/cups/model/`. La configuration d'imprimante YaST reconnaît ces modifications et régénère la base de données des fabricants et modèles. Par exemple, si vous ne possédez que des imprimantes PostScript, vous n'avez normalement besoin ni des fichiers PPD Foomatic du paquetage `cups-drivers`, ni des PPD Gimp-Print du paquetage `cups-drivers-stp`. Vous pouvez copier les fichiers PPD pour vos imprimantes PostScript directement vers `/usr/share/cups/model/` (s'ils n'existent pas déjà dans le paquetage `manufacturer-PPDs`) afin d'obtenir une configuration optimale de vos imprimantes.

Fichiers PPD CUPS dans le paquetage cups

Les fichiers PPD génériques dans le paquetage cups ont été complétés par des fichiers PPD Foomatic adaptés aux imprimantes PostScript Niveau 1 et Niveau 2 :

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

Fichiers PPD dans le paquetage cups-drivers

Normalement, le filtre d'impression Foomatic foomatic-rip est utilisé avec Ghostscript sur les imprimantes non-PostScript. Les fichiers PPD Foomatic ont les entrées *NickName: ... Foomatic/Ghostscript driver et *cupsFilter: ... foomatic-rip. Ces fichiers PPD se trouvent dans le paquetage cups-drivers.

YaST préfère un fichier PPD Foomatic, si un fichier PPD Foomatic avec l'entrée *NickName: ... Foomatic ... (recommended) correspond au modèle d'imprimante et si le paquetage manufacturer-PPDs ne contient aucun fichier PPD mieux adapté.

Fichiers PPD Gimp-Print dans le paquetage cups-drivers-stp

Au lieu d'utiliser foomatic-rip, vous pouvez employer le filtre CUPS rastertoprinter de Gimp-Print pour de nombreuses imprimantes non-PostScript. Ce filtre et les fichiers PPD Gimp-Print appropriés sont disponibles dans le paquetage cups-drivers-stp. Les fichiers PPD Gimp-Print PPD se trouvent dans /usr/share/cups/model/stp/ et ont les entrées *NickName: ... CUPS+Gimp-Print et *cupsFilter: ... rastertoprinter.

Fichiers PPD de fabricants d'imprimantes dans le paquetage manufacturer-PPDs

Le paquetage manufacturer-PPDs contient des fichiers PPD de fabricants d'imprimantes, commercialisés sous une licence suffisamment ouverte. Les imprimantes Post-

Script devraient être configurées avec le fichier PPD approprié du fabricant d'imprimantes, car ce fichier permet d'utiliser toutes les fonctions de l'imprimante PostScript. YaST préfère un fichier PPD émanant du paquetage `manufacturer-PPDs` si les conditions suivantes sont remplies :

- Le fabricant et le modèle déterminés au cours de la détection du matériel correspondent au fabricant et au modèle figurant dans un fichier PPD du paquetage `manufacturer-PPDs`.

- Le fichier PPD du paquetage `manufacturer-PPDs` est le seul qui convient au modèle d'imprimante ou il existe un fichier PPD Foomatic comportant une entrée `*NickName: ... Foomatic/Postscript (recommended)` qui correspond également au modèle de l'imprimante.

YaST n'utilise aucun fichier PPD du paquetage `manufacturer-PPDs` dans les cas suivants :

- Le fichier PPD du paquetage `manufacturer-PPDs` ne correspond pas au fabricant et au modèle. Cela peut se produire si le paquetage `manufacturer-PPDs` contient un seul fichier PPD pour des modèles similaires, par exemple, s'il n'existe pas de fichier PPD distinct pour chacun des modèles d'une série mais que le nom du modèle est spécifié sous la forme `Funprinter 1000 series` dans le fichier PPD.

- Le fichier PPD Foomatic PostScript n'est pas recommandé. Cela peut être dû au fait que le modèle d'imprimante ne fonctionne pas assez efficacement en mode PostScript, par exemple, il est possible que l'imprimante ne soit pas fiable dans ce mode car elle n'a pas suffisamment de mémoire, ou qu'elle soit trop lente, si le processeur n'est pas assez puissant. De plus, l'imprimante peut ne pas prendre en charge le format PostScript par défaut, par exemple quand cette prise en charge n'est disponible que sous forme de module facultatif.

Si un fichier PPD du paquetage `manufacturer-PPDs` convient à une imprimante PostScript, mais que YaST ne peut pas la configurer pour les raisons ci-dessus, sélectionnez manuellement le modèle d'imprimante concerné dans YaST.

31.7 Dépannage

Les sections suivantes décrivent certains des problèmes de matériel et de logiciel d'impression les plus fréquemment rencontrés, et proposent des solutions.

31.7.1 Imprimantes sans prise en charge d'un langage d'impression standard

Les imprimantes qui ne prennent en charge aucun langage d'impression courant et qui ne peuvent être gérées qu'à l'aide de séquences de contrôle spéciales sont appelées *imprimantes GDI*. Ces imprimantes fonctionnent uniquement avec les versions de système d'exploitation pour lesquelles le fabricant fournit un pilote. *GDI* est une interface de programmation développée par Microsoft pour les périphériques graphiques. Le problème réel n'est pas lié à l'interface de programmation, mais au fait que les imprimantes GDI ne peuvent être contrôlées qu'avec le langage d'impression propriétaire du modèle d'imprimante concerné.

Certaines imprimantes fonctionnent aussi bien en mode GDI qu'avec l'un des langages d'impression standard. Certains fabricants fournissent des pilotes propriétaires pour leurs imprimantes GDI. L'inconvénient des pilotes d'imprimantes propriétaires est que vous n'avez aucune garantie qu'ils fonctionnent avec votre système d'impression et qu'ils sont compatibles avec les différentes plates-formes matérielles. En revanche, les imprimantes qui prennent en charge un langage d'impression standard ne dépendent pas d'aucune version spécifique de système d'impression et d'aucune plate-forme matérielle particulière.

Au lieu de perdre du temps à tenter de faire fonctionner un pilote propriétaire sous Linux, il est souvent plus économique d'acheter une imprimante prise en charge. Cela élimine définitivement votre problème de pilote. Vous n'avez plus besoin d'installer et de configurer un pilote d'impression spécial, ni d'obtenir des mises à jour de ce pilote à la suite de nouvelles évolutions du système d'impression.

31.7.2 Aucun fichier PPD approprié disponible pour une imprimante PostScript

Si le paquetage `manufacturer-PPDs` ne contient aucun fichier PPD adapté à une imprimante PPD PostScript, il devrait être possible d'utiliser le fichier PPD du CD contenant le pilote du fabricant de l'imprimante ou de télécharger le fichier PPD adapté depuis le site Web du fabricant de l'imprimante.

Si le fichier PPD est fourni sous forme de fichier d'archive Zip (.zip) ou d'un fichier auto-extractible (`.exe`), décompressez-le à l'aide de la commande `unzip`. Tout d'abord, lisez le contrat de licence figurant dans le fichier PPD. Exécutez ensuite l'utilitaire `cupstestppd` pour vérifier si le fichier PPD est compatible avec la « Spécification de format de fichier de description d'imprimante PostScript Adobe, version 4.3 ». Si l'utilitaire retourne la valeur « FAIL », cela signifie que le fichier PPD contient des erreurs graves qui risquent de poser des problèmes sérieux. Les points problématiques indiqués par `cupstestppd` doivent être éliminés. Si nécessaire, demandez un fichier PPD adapté au fabricant de l'imprimante.

31.7.3 Ports parallèles

L'approche la plus sûre consiste à connecter l'imprimante en direct sur le premier port parallèle et de sélectionner les paramètres de port parallèle suivants dans le BIOS :

- Adresse d'E/S : `378` (hexadécimal)
- Interruption : non significatif
- Mode : `Normal`, `SPP` ou `Output Only (Sortie uniquement)`
- DMA : désactivé

Si l'imprimante ne peut pas être pilotée à partir du port parallèle malgré ces paramètres, entrez explicitement l'adresse d'E/S, conformément au paramètre du BIOS, sous la forme `0x378` dans `/etc/modprobe.conf`. Si deux ports parallèles sont définis sur les adresses d'E/S `378` et `278` (hexadécimal), entrez-les sous la forme `0x378,0x278`.

Si l'interruption 7 est libre, vous pouvez l'activer à l'aide de l'entrée présentée dans l'Exemple 31.1, « /etc/modprobe.conf : mode Interruption pour le premier port parallèle » (p. 529). Avant d'activer le mode Interruption, consultez le fichier /proc/interrupts pour connaître les interruptions déjà utilisées. Seules les interruptions en cours d'utilisation sont affichées. Cela peut changer en fonction des composants matériels qui sont actifs. L'interruption correspondant au port parallèle ne doit être utilisée par aucun autre périphérique. En cas de doute, utilisez le mode d'interrogation avec irq=none.

Exemple 31.1 */etc/modprobe.conf : mode Interruption pour le premier port parallèle*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

31.7.4 Connexion d'imprimantes réseau

Identification des problèmes réseau

Connectez l'imprimante directement sur l'ordinateur. Pour le test, configurez l'imprimante en tant qu'imprimante locale. Si elle fonctionne, cela signifie que les problèmes sont liés au réseau.

Vérification du réseau TCP/IP

Le réseau TCP/IP et la résolution des noms doivent fonctionner.

Vérification d'un périphérique `lpd` distant

Utilisez la commande suivante pour vérifier s'il est possible d'établir une connexion TCP avec un périphérique lpd (port 515) sur l'ordinateur *host* :

```
netcat -z host 515 && echo ok || echo failed
```

Si la connexion lpd échoue, cela signifie que lpd n'est pas actif ou qu'il existe des problèmes au niveau du réseau.

Loguez-vous en tant qu'utilisateur root, puis utilisez la commande suivante pour obtenir un rapport d'état (qui peut être très long) pour la file d'attente *queue* sur l'ordinateur distant *host*, à condition que le lpd concerné soit actif et que l'hôte accepte les requêtes :

```
echo -e "\004queue" \
  | netcat -w 2 -p 722 host 515
```

Si lpd ne répond pas, il est inactif ou il existe des problèmes réseau. Si lpd répond, cette réponse doit indiquer la cause du problème d'impression sur la file d'at-

tente `queue` sur l'ordinateur `host`. Si vous recevez une réponse comme celle de l'Exemple 31.2, « Message d'erreur de `lpd` » (p. 530), le problème est dû au `lpd` distant.

Exemple 31.2 *Message d'erreur de lpd*

```
lpd: your host does not have line printer access (l'hôte n'a pas accès à
l'imprimante en ligne)
lpd: queue does not exist (file d'attente inexistante)
printer: spooling disabled (spouling désactivé)
printer: printing disabled (impression désactivée
```

Test d'un cupsd distant

Par défaut, le serveur réseau CUPS doit diffuser ses files d'attente toutes les 30 secondes sur le port UDP `631`. Ainsi, vous pouvez utiliser la commande suivante pour tester la présence d'un serveur réseau CUPS sur le réseau.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Si un serveur réseau CUPS qui diffuse des données existe sur le réseau, la sortie doit apparaître comme dans l'Exemple 31.3, « Diffusion à partir du serveur réseau CUPS » (p. 530).

Exemple 31.3 *Diffusion à partir du serveur réseau CUPS*

```
ipp://host.domain:631/printers/queue
```

La commande suivante permet de tester si une connexion TCP peut être établie avec `cupsd` (port `631`) sur l'ordinateur *`host`* :

```
netcat -z host 631 && echo ok || echo failed
```

S'il est impossible d'établir la connexion à `cupsd`, ce dernier est inactif ou il existe des problèmes au niveau du réseau. La commande `lpstat -h host -l -t` retourne un rapport d'état (parfois très long) concernant toutes les files d'attente de l'ordinateur *`host`*, à condition que `cupsd` soit actif et que l'hôte accepte les requêtes.

Vous pouvez utiliser la commande suivante pour tester si la file d'attente *`queue`* sur l'ordinateur *`host`* accepte un travail d'impression uniquement constitué d'un seul caractère de retour chariot. Rien ne doit être imprimé. Parfois, l'imprimante éjecte une page vide.

```
echo -en "\r" \
  | lp -d queue -h host
```

Dépannage d'une imprimante réseau ou d'un boîtier serveur d'impression

Les spouleurs qui s'exécutent dans un boîtier serveur d'impression posent parfois des problèmes lorsqu'ils doivent gérer un grand nombre de travaux d'impression. Comme le spouleur figurant dans le boîtier serveur d'impression est responsable de ces problèmes, vous ne pouvez rien faire. Vous pouvez toutefois contourner le spouleur du boîtier serveur d'impression en pilotant l'imprimante connectée au serveur d'impression directement via un socket TCP. Voir Section 31.4.2, « Imprimantes réseau » (p. 516).

Ainsi, le boîtier serveur d'impression devient un simple convertisseur des divers formats de transmission de données (réseau TCP/IP et connexion à l'imprimante locale). Pour utiliser cette méthode, vous devez connaître le port TCP du boîtier serveur d'impression. Si l'imprimante est connectée au boîtier serveur d'impression et que vous la mettez sous tension, vous pouvez généralement déterminer ce port TCP avec l'utilitaire `nmap` du paquetage `nmap`, peu de temps après avoir mis en route le boîtier serveur d'impression. Par exemple, la commande `nmap` *`adresse-IP`* peut fournir la sortie suivante pour un boîtier serveur d'impression :

```
Port        State        Service
23/tcp      open         telnet
80/tcp      open         http
515/tcp     open         printer
631/tcp     open         cups
9100/tcp    open         jetdirect
```

Cette sortie indique que l'imprimante connectée au boîtier serveur d'impression peut être pilotée via le socket TCP sur le port `9100`. Par défaut, `nmap` vérifie uniquement quelques ports courants, répertoriés dans `/usr/share/nmap/nmap-services`. Pour vérifier tous les ports possibles, utilisez la commande `nmap -p` *`port_début-port_fin adresse-IP`*. Le traitement peut être assez long. Pour plus d'informations, consultez la page de manuel `nmap`.

Entrez une commande similaire à :

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

pour envoyer des chaînes de caractères ou des fichiers directement au port concerné, afin de vérifier s'il est possible de piloter l'imprimante sur ce port.

31.7.5 Impressions défectueuses sans message d'erreur

Pour le système d'impression, l'impression est terminée lorsque l'interface dorsale CUPS a fini de transférer les données vers le destinataire (imprimante). Si le traitement ultérieur sur le destinataire échoue, par exemple, si l'imprimante ne peut pas imprimer des données propres à l'imprimante, le système d'impression ne le détecte pas. Si l'imprimante ne peut pas imprimer de données propres à l'imprimante, sélectionnez un autre fichier PPD, mieux adapté à votre imprimante.

31.7.6 Files d'attente désactivées

Si le transfert des données vers le destinataire échoue complètement après plusieurs tentatives, l'interface dorsale CUPS, comme `usb` ou `socket`, signale une erreur au système d'impression (`cupsd`). L'interface dorsale décide alors si de nouvelles tentatives doivent être lancées (et détermine leur nombre) jusqu'à ce que le transfert soit considéré comme impossible. Comme toute tentative supplémentaire est vouée à l'échec, `cupsd` désactive l'impression pour la file d'attente concernée. Après avoir éliminé la cause du problème, l'administrateur système doit réactiver l'impression, à l'aide de la commande `/usr/bin/enable`.

31.7.7 Navigation dans CUPS : suppression de travaux d'impression

Si un serveur réseau CUPS diffuse ses files d'attente aux hôtes clients par navigation et qu'un utilitaire `cupsd` local approprié est actif sur les hôtes clients, le client `cupsd` accepte les travaux provenant des applications et les transfère vers `cupsd` sur le serveur. Lorsque `cupsd` accepte un travail d'impression, il lui affecte un nouveau numéro. Par conséquent, le numéro de travail sur l'hôte client est différent de celui défini sur le serveur. Comme un travail d'impression est généralement transféré immédiatement, vous ne pouvez pas le modifier avec le numéro de travail déterminé sur l'hôte client, car le client `cupsd` considère ce travail comme terminé dès qu'il a été transféré vers `cupsd` sur le serveur.

Pour supprimer le travail d'impression sur le serveur, utilisez une commande comme `lpstat -h print-server -o` pour déterminer le numéro du travail sur le ser-

veur ; cela n'est possible que si le serveur n'a pas terminé le travail (c'est-à-dire, ne l'a pas encore envoyé à l'imprimante). Avec ce numéro de travail, vous pouvez supprimer le travail d'impression sur le serveur :

```
cancel -h print-server queue-jobnnumber
```

31.7.8 Travaux d'impression défectueux et erreurs de transfert de données

Les travaux d'impression restent dans les files d'attente et l'impression reprend si vous éteignez et rallumez l'imprimante, ou si vous redémarrez l'ordinateur pendant l'impression. Les travaux d'impression défectueux doivent être supprimés de la file d'attente avec la commande `cancel`.

Si un travail d'impression est défectueux, ou s'il se produit une erreur de communication entre l'hôte et l'imprimante, celle-ci imprime une multitude de feuilles aux caractères illisibles car elle est incapable de traiter correctement les données. Pour résoudre ce problème, procédez comme suit :

1. Pour arrêter l'impression, ôtez tout le papier des imprimantes jet d'encre ou ouvrez tous les bacs d'alimentation des imprimantes laser. Les imprimantes haut de gamme comportent un bouton qui annule l'impression en cours.

2. Le travail d'impression peut demeurer dans la file d'attente, car les travaux ne sont supprimés que lorsqu'ils ont été complètement envoyés à l'imprimante. Utilisez la commande `lpstat -o` ou `lpstat -h` *`serveur-impression`* `-o` pour connaître la file d'attente qui est en train d'imprimer. Supprimez le travail d'impression avec la commande `cancel` *`file-attente-numéro-travail`* ou la commande `cancel -h` *`serveur-impression file-attente-numéro-travail`*.

3. Certaines données risquent encore d'être transférées vers l'imprimante, même si le travail d'impression a été supprimé de la file d'attente. Vérifiez si un processus d'interface dorsale CUPS est encore en cours d'exécution pour la file d'attente concernée et arrêtez-le. Par exemple, pour une imprimante connectée au port parallèle, vous pouvez utiliser la commande `fuser -k /dev/lp0` pour terminer tous les processus qui continuent d'accéder à l'imprimante (ou plus précisément, au port parallèle).

4 Réinitialisez complètement l'imprimante en l'éteignant pendant un moment. Insérez ensuite du papier et allumez l'imprimante.

31.7.9 Débogage du système d'impression CUPS

Utilisez la procédure générique suivante pour localiser les problèmes du système d'impression CUPS :

1 Définissez `LogLevel debug` dans `/etc/cups/cupsd.conf`.

2 Arrêtez `cupsd`.

3 Supprimez `/var/log/cups/error_log*` pour éviter d'avoir à effectuer des recherches dans des fichiers journaux très volumineux.

4 Démarrez `cupsd`.

5 Répétez l'action qui a déclenché le problème.

6 Consultez les messages dans `/var/log/cups/error_log*` pour identifier la cause du problème.

31.7.10 Pour plus d'informations

Vous trouverez la solution à de nombreux problèmes particuliers dans la base de données de support. Pour tout problème d'imprimante, consultez les articles de la base de données de support intitulés *Installation d'une imprimante* et *Configurer une imprimante depuis SUSE Linux 9.2*, que vous trouverez en saisissant le mot-clé *imprimante*.

32 Le système Hotplug

Le système Hotplug contrôle l'initialisation de la plupart des périphériques d'un ordinateur. Il ne s'utilise pas seulement avec les périphériques qui peuvent être ajoutés et retirés en cours de fonctionnement, mais avec tous les périphériques qui sont détectés lors du démarrage du système. Il est étroitement associé avec le système de fichiers `sysfs` et l'utilitaire `udev`, décrits au Chapitre 33, *Noeuds de périphériques dynamiques avec `udev`* (p. 543).

Jusqu'au démarrage du kernel, seuls les périphériques indispensables (système de bus, disques d'amorçage et claviers) sont initialisés. Le kernel déclenche les événements hotplug pour tous les périphériques détectés. Le démon `udevd` écoute ces événements et exécute `udev` pour créer le noeud de périphérique et configurer le périphérique. Pour les périphériques qui ne peuvent être détectés automatiquement, tels que les anciennes cartes ISA, une configuration statique est utilisée.

Hormis certaines exceptions historiques, la plupart des périphériques sont initialisés dès qu'ils sont accessibles, soit lors du démarrage du système, soit lorsqu'ils sont connectés à chaud. Au cours de l'initialisation, les interfaces sont enregistrées dans le kernel. Cet enregistrement déclenche d'autres événements hotplug, qui provoquent la configuration automatique l'interface appropriée.

Dans les versions précédentes de SUSE Linux, un jeu statique de données de configuration était utilisé comme base pour l'initialisation des périphériques. Tous les événements hotplug étaient gérés par des scripts séparés, nommés agents. Avec cette version de SUSE Linux, le sous-système hotplug est intégré à udev, les règles udev fournissant la fonctionnalité des anciens agents hotplug.

Les paramètres généraux du sous-système hotplug se trouvent dans `/etc/sysconfig/hotplug`. Toutes les variables sont commentées. La configuration générale du périphérique s'effectue en fonction des règles correspondantes dans `/etc/udev/rules.d` (voir Chapitre 33, *Noeuds de périphériques dynamiques avec* `udev` (p. 543)). Les fichiers de configuration spécifiques de certains périphériques se trouvent dans `/etc/sysconfig/hardware`. Le rappel d'événement hotplug utilisé dans les versions précédentes de SUSE Linux, `/proc/sys/kernel/hotplug`, est généralement vide car `udevd` reçoit les messages hotplug via un socket netlink.

32.1 Périphériques et interfaces

Le système hotplug configure non seulement les périphériques, mais aussi les interfaces. En règle générale, un périphérique est connecté à un bus et fournit la fonctionnalité requise pour une interface. Une interface représente l'ensemble des fonctions, visibles par l'utilisateur, d'un périphérique ou d'un sous-ensemble d'un périphérique. Un périphérique nécessite généralement un pilote, prenant la forme de modules de kernel, pour fonctionner correctement. En outre, un pilote de plus haut niveau peut être nécessaire pour fournir l'interface à l'utilisateur. Les interfaces sont le plus souvent représentées par les noeuds de périphérique créés par `udev`. Pour comprendre le concept global, il est essentiel d'appréhender la distinction entre les périphériques et les interfaces.

Les périphériques entrés dans le système de fichiers `sysfs` se trouvent sous `/sys/devices`. Les interfaces se trouvent sous `/sys/class` ou sous `/sys/block`. Toutes les interfaces de `sysfs` doivent avoir un lien vers leur périphérique. Cependant, il existe encore des pilotes qui n'ajoutent pas automatiquement ce lien. Sans ce lien, Linux ne sait pas à quel périphérique appartient l'interface et ne trouve aucune configuration appropriée.

L'accès aux périphériques s'effectue au moyen d'une description. Il peut s'agir du chemin du périphérique spécifié dans `sysfs` (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`), d'une description du point de connexion (`bus-pci-0000:02:00.0`), d'un ID individuel (`id-32311AE03FB82538`) ou de toute autre information similaire. Auparavant, l'accès aux interfaces s'effectuait par leur nom. Ces noms représentaient une simple numérotation des périphériques existants et étaient susceptibles de changer lorsque l'on ajoutait ou supprimait des périphériques.

L'accès aux interfaces peut également s'effectuer à l'aide d'une description du périphérique associé. Généralement, le contexte indique si la description se réfère au

périphérique lui-même ou à son interface. Exemples de périphériques, d'interfaces et de descriptions :

Carte réseau PCI
Périphérique connecté au bus PCI (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` ou `bus-pci-0000:02:00.0`) et doté d'une interface réseau (`eth0`, `id-00:0d:60:7f:0b:22` ou `bus-pci-0000:02:00.0`). L'interface réseau est utilisée par les services réseau ou connectée à un périphérique réseau virtuel, tel qu'un tunnel ou un VLAN, lui-même connecté à une interface.

Contrôleur SCSI PCI
Périphérique (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` ou `bus-scsi-1:0:0:0`) qui rend plusieurs interfaces physiques disponibles sous la forme d'un bus (`/sys/class/scsi_host/host1`).

Disque dur SCSI
Périphérique (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` ou `bus-scsi-1:0:0:0`) doté de plusieurs interfaces (`/sys/block/sda*`).

32.2 Evénements hotplug

Chaque périphérique et chaque interface a un *événement hotplug* associé, qui est traité par `udev`. Le kernel déclenche un événement hotplug lorsqu'un lien à un périphérique est établi ou supprimé ou lorsqu'un pilote enregistre ou supprime une interface. À compter de SUSE Linux 9.3, `udevd` reçoit et traite les événements hotplug. Soit `udevd` écoute directement les messages netlink à partir du kernel, soit `/sbin/udevsend` doit être spécifié dans `/proc/sys/kernel/hotplug`. `udevd` configure le périphérique selon un ensemble de règles (voir le Chapitre 33, *Noeuds de périphériques dynamiques avec `udev`* (p. 543)).

32.3 Configuration des périphériques hotplug

Les agents hotplug ne sont plus autorisés depuis SUSE Linux 10.0. Dorénavant, la configuration de tous les périphériques doit s'effectuer via les règles udev. `udev` offre

une règle de compatibilité pour appeler les agents personnalisés existants. Cependant, il est recommandé d'envisager la conversion des agents personnalisés en règles udev.

Un agent hotplug est un programme exécutable qui effectue des actions appropriées à un événement. Les agents des événements de périphériques se trouvent dans les répertoires `/etc/hotplug.d/` *`nom de l'événement`* et `/etc/hotplug.d/default`. Tous les programmes contenus dans ces répertoires et ayant le suffixe `.hotplug` sont exécutés par ordre alphabétique.

Pour faciliter la configuration des périphériques, il suffit généralement de charger un module du kernel. Dans certains cas, il est cependant nécessaire d'appeler des commandes supplémentaires pour assurer la configuration correcte du périphérique. Dans SUSE Linux, cette configuration est généralement gérée par des règles udev. Cependant, si une configuration personnalisée de périphérique est requise, celle-ci est effectuée par `/sbin/hwup` ou par `/sbin/hwdown`. Ces programmes recherchent une configuration appropriée au périphérique dans le répertoire `/etc/sysconfig/hardware` et l'appliquent. Par exemple, pour empêcher l'initialisation d'un périphérique spécifique, créez un fichier de configuration portant un nom approprié et réglez le mode de démarrage sur `manual` ou sur `off`. Si `/sbin/hwup` ne trouve pas de configuration, il recherche la variable d'environnement `MODALIAS`. Si elle existe, `modprobe` charge automatiquement le module correspondant. La variable `MODALIAS` est générée automatiquement par les événements hotplug du kernel pour les périphériques nécessitant le chargement d'un module. Pour plus d'informations, consultez la Section 32.4, « Chargement automatique des modules » (p. 540). Pour plus d'informations sur `/sbin/hwup` consultez le fichier `/usr/share/doc/packages/sysconfig/README` et la page de manuel `man hwup`.

Avant l'appel des agents de l'interface, `udev` génère généralement un noeud de périphérique accessible par le système. `udev` active l'attribution de noms persistants aux interfaces. Pour plus de détails, reportez-vous au Chapitre 33, *Noeuds de périphériques dynamiques avec `udev`* (p. 543). Les interfaces sont ensuite configurées en fonction des règles udev appropriées. Les procédures relatives à certaines interfaces sont décrites ci-dessous.

32.3.1 Activation d'interfaces réseau

Les interfaces réseau sont initialisées à l'aide de `/sbin/ifup` et désactivées avec `/sbin/ifdown`. Des détails sont fournis dans le fichier `/usr/share/doc/packages/sysconfig/README` et dans la page de manuel `ifup`.

Sur un ordinateur qui possède des périphériques réseau utilisant plusieurs pilotes différents, la désignation d'une interface peut changer si un autre pilote est chargé plus vite lors du démarrage du système. SUSE Linux tente de conserver la numérotation persistante (les périphériques conservent le nom d'interface qui leur a été attribué au cours de la configuration). L'attribution des désignations s'effectue via des règles udev. Pour la modifier par la suite, il faut modifier les règles udev.

Cependant, la meilleure solution consiste à utiliser des désignations d'interfaces persistantes. Vous pouvez spécifier les noms des interfaces dans les fichiers de configuration. Vous trouverez la description détaillée de cette méthode dans le fichier `/usr/share/doc/packages/sysconfig/README`. Depuis SUSE Linux 9.3, udev gère également les interfaces réseau, bien que celles-ci ne soient pas des noeuds de périphérique. Cela permet d'utiliser les noms d'interface persistants d'une façon plus standardisée.

32.3.2 Activation de périphériques de stockage

Les interfaces des périphériques de stockage doivent être montées pour que ces périphériques soient accessibles. Le montage est entièrement automatisable et pré configurable. De surcroît, SUSE Linux distingue les périphériques système et des périphériques utilisateur. Pour monter automatiquement un périphérique système, il est impératif de créer une entrée dans `/etc/fstab`. Les périphériques utilisateur sont gérés via `hal` par défaut. Si un périphérique utilisateur requiert une configuration différente, ce périphérique peut être entré dans `/etc/fstab`. Il est également possible de modifier la gestion d'un périphérique dans `hal`. Pour plus d'informations sur `hal`, lisez le document `/usr/share/doc/packages/hal/hal-spec.html`.

Il est recommandé d'utiliser des noms de périphériques persistants, car les noms de périphériques traditionnels peuvent changer selon la séquence d'initialisation. Pour plus d'informations sur les noms de périphérique persistants, reportez-vous au Chapitre 33, *Noeuds de périphériques dynamiques avec `udev`* (p. 543).

32.4 Chargement automatique des modules

Si /sbin/hwup ne parvient pas à détecter un fichier de configuration, modprobe recherche un module correspondant en fonction du contenu de la variable d'environnement MODALIAS. Cette variable d'environnement est générée par le kernel pour l'événement hotplug correspondant. Pour utiliser un pilote différent du pilote standard du kernel, il faut créer un fichier de configuration du matériel approprié dans /etc/sysconfig/hardware.

32.5 La commande de démarrage coldplug

La commande boot.coldplug est responsable de l'initialisation de tous les périphériques qui n'ont pas été configurés lors du démarrage. Elle appelle hwup pour chaque configuration de périphérique statique désignée comme /etc/sysconfig/hardware/hwcfg-static-*. Ensuite, elle relit tous les événements stockés dans /lib/klibc/events pour initialiser tous les périphériques.

32.6 Analyse des erreurs

32.6.1 Fichiers journaux

Sauf indication contraire, hotplug n'envoie que quelques messages importants à syslog. Pour obtenir davantage d'informations, définissez la variable HOTPLUG_DEBUG contenue dans le fichier /etc/sysconfig/hotplug sur yes. Si vous définissez cette variable sur la valeur max, chaque commande de shell est consignée pour tous les scripts hotplug. Le fichier /var/log/messages dans lequel syslog stocke tous les messages devient beaucoup plus grand. syslog étant lancé après hotplug et coldplug au cours du processus d'amorçage, il est toutefois possible que le premier messages ne soit pas consigné. Si vous avez besoin d'enregistrer

ces messages, indiquez un fichier journal différent via la variable HOTPLUG_SYSLOG. Vous trouverez des informations sur ce sujet dans /etc/sysconfig/hotplug.

32.6.2 Problèmes de démarrage

Si un ordinateur se bloque au cours du processus de démarrage, désactivez hotplug ou coldplug en entrant NOHOTPLUG=yes ou NOCOLDPLUG=yes à l'invite de démarrage. Du fait de la désactivation de hotplug, le kernel n'émettra pas d'événements hotplug. Pendant l'exécution, vous pouvez activer hotplug en entrant la commande /etc/init.d/boot.hotplug start. Tous les événements générés jusqu'à ce moment seront alors diffusés et traités. Pour rejeter les événements en file d'attente, entrez d'abord /bin/true dans /proc/sys/kernel/hotplug et réinitialisez l'entrée à /sbin/hotplug après quelque temps. Du fait de la désactivation de coldplug, les configurations statiques ne sont pas appliquées. Pour appliquer les configurations statiques, entrez ultérieurement /etc/init.d/boot.coldplug start.

Pour savoir si un module particulier chargé par hotplug est responsable du problème, entrez HOTPLUG_TRACE=<N> à l'invite de démarrage. Les noms de tous les modules à charger sont d'abord affichés à l'écran, puis les modules sont chargés après *N* secondes. Vous ne pouvez pas intervenir lors de ce processus.

32.6.3 Enregistreur d'événements

Le script /sbin/hotplugeventrecorder est exécuté pour chaque événement par une règle udev. S'il existe un répertoire /events, tous les événements hotplug sont stockés comme des fichiers dans ce répertoire. Ainsi, les événements peuvent être régénérés à des fins de test. Si ce répertoire n'existe pas, aucune donnée n'est enregistrée.

Noeuds de périphériques dynamiques avec udev

33

Linux kernel 2.6 présente une nouvelle solution d'espace utilisateur pour les répertoires de périphériques dynamiques /dev avec des désignations de périphérique persistantes : udev. Cette solution ne fournit que les fichiers ou les périphériques réellement présents. Elle crée ou supprime les fichiers du noeud de périphérique généralement situés dans le répertoire /dev et peut renommer les interfaces réseau. La implémentation précédente d'un /dev dynamique avec devfs a été remplacée par udev.

Traditionnellement, les noeuds de périphériques étaient stockés dans le répertoire /dev sur les systèmes Linux. Il y avait un noeud pour chaque type de périphérique possible, qu'il existe ou non dans le système. En conséquence, ce répertoire contenait des milliers de fichiers inutilisés. Avant qu'un nouveau sous-système ou un nouveau périphérique du kernel puisse être utilisé, les noeuds correspondants devaient être créés avec une application spéciale. Le système de fichiers devfs a apporté une amélioration significative car seuls les périphériques qui existaient réellement et étaient connus du kernel se voyaient attribuer un noeud de périphérique dans /dev.

udev introduit un nouveau moyen de créer des noeuds de périphériques. Le kernel exporte son état interne dans sysfs et, chaque fois qu'un périphérique est reconnu par le kernel, il met à jour les informations dans sysfs et envoie un événement à l'espace utilisateur. Grâce aux informations rendues disponibles par sysfs, udev fait correspondre une syntaxe de règle simple avec les attributs du périphérique puis crée ou supprime les noeuds de périphériques correspondants.

L'utilisateur n'a pas besoin de créer de règle udev pour les nouveaux périphériques. Si un périphérique est connecté, le noeud de périphérique correspondant est créé automatiquement. Toutefois, les règles introduisent la possibilité de définir une stratégie de désignation de périphérique. Ceci permet en outre de remplacer un nom de

périphérique crypté par un nom facile à mémoriser et d'avoir des noms de périphérique persistants lorsque deux périphériques de même type ont été connectés en même temps.

Supposons que l'on ait deux imprimantes, une imprimante laser couleur de haute qualité et une imprimante à jet d'encre noir et blanc, toutes deux connectées par USB. Elles apparaissent en tant que `/dev/usb/lpX`, où X est un numéro dépendant de l'ordre dans lequel elles ont été connectées. En utilisant udev, vous pouvez créer des règles udev personnalisées pour nommer une imprimante `/dev/lasercouleur` et l'autre `/dev/jetd'encre`. Du fait que ces noeuds de périphériques sont créés par udev en fonction des caractéristiques du périphérique, ils pointent toujours vers le bon périphérique, quel que soit l'ordre ou l'état de la connexion.

33.1 Création de règles

Avant qu'`udev` ne crée des noeuds de périphériques sous `/dev`, il lit tous les fichiers de `/etc/udev/rules.d` dont le suffixe est `.rules` dans l'ordre alphabétique. La première règle qui correspond à un périphérique est utilisée, même si d'autres peuvent également s'appliquer. Des commentaires sont introduits par le signe `#`. Les règles prennent la forme suivante :

```
key, [key,...] NAME [, SYMLINK]
```

Au moins une clé doit être spécifiée. En effet, les règles sont assignées aux périphériques sur la base de ces clés. Il est également essentiel de spécifier un nom. Le noeud de périphérique créé dans `/dev` porte ce nom. Le paramètre symlink facultatif permet aux noeuds d'être créés à d'autres endroits. Une règle pour une imprimante peut avoir la forme suivante :

```
BUS=="usb", SYSFS{serial}=="12345", NAME="lp_hp", SYMLINK+="printers/hp"
```

Dans cet exemple, il y a deux clés, `BUS` et `SYSFS{serial}`. `udev` compare le numéro de série à celui du périphérique connecté au bus USB. Pour assigner le nom `lp_hp` au périphérique du répertoire `/dev`, toutes les clés doivent être identiques. De plus, un lien symbolique `/dev/printers/hp`, qui fait référence au noeud de périphérique, est créé. En même temps, le répertoire `printers` est créé automatiquement. Les tâches d'impression peuvent être envoyées à `/dev/printers/hp` ou à `/dev/lp_hp`.

33.2 Substitution d'espaces réservés

Les paramètres NAME et SYMLINK permettent l'utilisation d'espaces réservés pour remplacer des valeurs spéciales. Un exemple simple illustre cette procédure :

```
BUS=="usb", SYSFS{vendor}=="abc", SYSFS{model}=="xyz", NAME="camera%n"
```

L'opérateur %n dans le nom est remplacé par le numéro du périphérique appareil photo, tel que camera0 ou camera1. %k est un autre opérateur utile qui est remplacé par le nom du périphérique standard du kernel, par exemple hda1. Vous pouvez également appeler un programme externe dans des règles udev et utiliser la chaîne qui est renvoyée dans les valeurs NAME et SYMLINK. La liste complète des espaces réservés possibles est décrite dans la page de manuel udev.

33.3 Correspondance de modèle dans les clés

Dans les clés des règles udev, vous pouvez utiliser la correspondance de modèle de style shell, nommée joker. Par exemple, le caractère * peut être utilisé comme espace réservé pour n'importe quel caractère. Quant au caractère ?, il peut être utilisé pour précisément un caractère arbitraire.

```
KERNEL="ts*", NAME="input/%k"
```

Cette règle assigne le nom de kernel standard du répertoire standard à un périphérique dont la désignation commence par les lettres « ts ». Pour plus d'informations sur l'utilisation de la correspondance de modèle dans les règles udev, consultez la page de manuel udev.

33.4 Sélection des clés

Pour identifier un périphérique de façon unique et distinguer plusieurs périphériques les uns des autres, une propriété unique est essentielle pour qu'une règle udev fonctionne. Voici quelques exemples de clés standard :

SUBSYSTEM
: Sous-système dont fait partie de périphérique

BUS

Type de bus du périphérique

KERNEL

Nom du périphérique utilisé par le kernel

ID

Numéro du périphérique sur le bus (par exemple, ID du bus PCI)

SYSFS{...}

Attributs de périphérique sysfs, tels que étiquette, fournisseur ou numéro de série

Les clés `SUBSYSTEM` et `ID` peuvent être utiles, mais généralement les clés `BUS`, `KERNEL` et `SYSFS{...}` sont utilisées. La configuration `udev` fournit également des clés qui appellent des scripts externes et en évaluent les résultats. Vous trouverez des informations à ce sujet dans la page de manuel `udev`.

Le système de fichiers `sysfs` présente des informations concernant le matériel dans une arborescence de répertoire. Chaque fichier ne contient généralement qu'un élément d'information, tel que le nom du périphérique, le fournisseur ou le numéro de série. Chacun de ces fichiers peut être utilisé pour correspondre à une clé. Toutefois, pour utiliser plusieurs clés `SYSFS` dans une règle, vous ne pouvez utiliser que des fichiers d'un même répertoire comme valeurs de clé. L'outil `udevinfo` peut aider à trouver des valeurs de clé utiles et uniques.

Vous devez trouver un sous-répertoire de `/sys` qui fasse référence au périphérique correspondant et qui contienne un fichier `dev`. Ces répertoires se trouvent tous sous `/sys/block` ou sous `/sys/class`. S'il existe déjà un noeud pour ce périphérique, `udevinfo` peut trouver le bon sous-répertoire à votre place. La commande `udevinfo -q path -n /dev/sda` génère `/block/sda`. Cela signifie que le répertoire désiré est `/sys/block/sda`. Appelez maintenant `udevinfo` avec la commande `udevinfo -a -p /sys/block/sda`. Les deux commandes peuvent également se combiner, comme dans ``udevinfo -a -p `udevinfo -q path -n /dev/sda` ``. Voici un extrait du résultat :

```
BUS=="scsi"
ID=="0:0:0:0"
SYSFS{detach_state}=="0"
SYSFS{type}=="0"
SYSFS{max_sectors}=="240"
SYSFS{device_blocked}=="0"
SYSFS{queue_depth}=="1"
SYSFS{scsi_level}=="3"
```

```
SYSFS{vendor}==" "
SYSFS{model}=="USB 2.0M DSC"
SYSFS{rev}=="1.00"
SYSFS{online}=="1"
```

À partir des informations générées, recherchez les clés appropriées qui ne changent pas. N'oubliez pas que vous ne pouvez pas utiliser de clés de répertoires différents dans une même règle.

33.5 Noms persistants pour les périphériques de stockage de masse

SUSE Linux est livré avec des règles prédéfinies qui vous permettent toujours d'attribuer les mêmes désignations aux disques durs et autres périphériques de stockage de masse, quel que soit l'ordre dans lequel ils sont initialisés. Des attributs de périphérique uniques, tels que les numéros de série des matériels, les UUID ou les étiquettes de systèmes de fichiers, peuvent être lus avec de petits programmes d'aide qui accompagnent udev. Ces programmes d'aide fournissent des informations spécifiques sur le périphérique pour le traitement par la règle udev. Comme exemple simplifié, la première règle importe les valeurs recueillies à partir du périphérique SCSI dans l'environnement udev. La seconde règle utilise les valeurs importées pour créer un lien symbolique persistant.

```
KERNEL="sd*[!0-9]", IMPORT="/sbin/scsi_id -g -x -s $p -d %N"
KERNEL="sd*[!0-9]", SYMLINK+="$env{ID_TYPE}/by-id/$env{ID_BUS}-$env{ID_SERIAL}"
```

Dès qu'un pilote de périphérique de stockage de masse a été chargé, il enregistre tous les disques durs disponibles dans le kernel. Chacun d'entre eux déclenche un événement de blocage hotplug qui appelle `udev`. `udev` lit ensuite les règles pour déterminer si un lien symbolique doit être créé.

Si le pilote est chargé via `initrd`, les événements hotplug sont perdus. Toutes les informations sont toutefois stockées dans `sysfs`. L'utilitaire `udevstart` recherche tous les fichiers de périphérique sous `/sys/block` et `/sys/class`, puis démarre `udev`.

Il existe également un script de démarrage `boot.udev`, qui recrée tous les noeuds de périphériques au cours du processus d'amorçage. Le script de démarrage doit cependant

être activé par l'intermédiaire de l'éditeur de niveau d'exécution YaST ou avec la commande `insserv boot.udev`.

Systèmes de fichiers sous Linux 34

Linux prend en charge un certain nombre de systèmes de fichiers différents. Ce chapitre présente un bref tour d'horizon des systèmes de fichiers Linux les plus connus, en insistant sur leur principe de conception, leurs avantages et leurs domaines d'application. Quelques informations complémentaires sur LFS (Large File Support,prise en charge des gros fichiers) sous Linux sont également offertes.

34.1 Terminologie

métadonnées
: Une structure de données interne à un système de fichiers qui garantit que toutes les données sur le disque sont correctement organisées et accessibles. Il s'agit essentiellement des « données concernant les données ». Pratiquement chaque système de fichiers a sa propre structure de métadonnées, ce qui explique en partie la raison pour laquelle les systèmes de fichiers affichent des caractéristiques de performances différentes. Il est particulièrement important de conserver intactes les métadonnées car, sinon, toutes les données présentes sur le système de fichiers pourraient devenir inaccessibles.

inode
: Les inodes contiennent diverses informations sur un fichier, dont sa taille, le nombre de liens, la date, la date et l'heure de création, les modifications et l'accès ainsi que les pointeurs sur les blocs du disque dans lesquels le contenu des fichiers est effectivement enregistré.

journal

Dans le contexte d'un système de fichiers, un journal est une structure sur disque contenant une sorte de fichier journal dans lequel le système de fichiers enregistre ce qui est sur le point de changer dans les métadonnées du système de fichiers. La journalisation réduit considérablement le temps de restauration d'un système Linux, parce qu'il supprime le processus de recherche très long qui vérifie le système de fichiers complet au démarrage du système. À la place, seul le journal est relu.

34.2 Les principaux systèmes de fichiers sous Linux

Contrairement à il y a deux ou trois ans, on ne choisit plus un système de fichiers pour Linux en quelques secondes (Ext2 ou ReiserFS ?). Les noyaux à partir de la version 2.4 proposent une grande variété de systèmes de fichiers. Vous trouverez ci-après une vue d'ensemble des grands principes de fonctionnement de ces systèmes de fichiers et les avantages qu'ils offrent.

Il est très important de considérer qu'il ne peut pas y avoir un système de fichiers qui convienne le mieux à tous les types d'applications. Chaque système de fichiers a ses points forts et ses faiblesses, qu'il faut prendre en compte. Quoi qu'il en soit, même le système de fichiers le plus sophistiqué ne peut pas remplacer une stratégie de sauvegarde raisonnable.

Les termes « intégrité des données » et « cohérence des données », lorsque utilisés dans ce chapitre, ne font pas référence à la cohérence des données de l'espace utilisateur (les données que votre application écrit sur ses fichiers). C'est l'application elle-même qui doit assurer la cohérence de ces données.

IMPORTANT: Configurer les systèmes de fichiers

Sauf indication contraire dans ce chapitre, toutes les étapes requises pour configurer ou changer des partitions et des systèmes de fichiers peuvent avoir lieu à l'aide du module de YaST.

34.2.1 ReiserFS

Officiellement, une des fonctionnalités phares de la version 2.4 du noyau, ReiserFS était disponible sous forme de correctif de noyau pour les noyaux SUSE 2.2.x depuis la version 6.4 de SUSE Linux. ReiserFS a été conçu par Hans Reiser et l'équipe de développement Namesys. ReiserFS a prouvé qu'il était une puissante alternative à l'ancien Ext2. Ses principaux atouts sont : une meilleure gestion de l'espace disque, de meilleures performances d'accès aux disques et une restauration plus rapide après une panne.

Les points forts de ReiserFS, de manière plus détaillée, sont :

Une meilleure gestion de l'espace disque
: Dans ReiserFS, toutes les données sont organisées dans une structure dénommée arbre équilibré B^*. Cette structure arborescente contribue à une meilleure gestion de l'espace disque car des petits fichiers peuvent être enregistrés directement dans les feuilles de l'arbre B^* au lieu de l'être à d'autres endroits en se contentent de tenir à jour un pointeur sur l'emplacement réel du disque. En plus de cela, le stockage n'est pas alloué en blocs de 1 ou de 4 ko, mais en portions de la taille exacte nécessaire. Un autre avantage se situe dans l'allocation dynamique des inodes. Ce comportement confère au système de fichiers une plus grande flexibilité par rapport aux systèmes de fichiers classiques, comme Ext2, dans lesquels il faut spécifier la densité d'inodes au moment où l'on crée le système de fichiers.

Meilleures performances d'accès aux disques
: Pour de petits fichiers, les données des fichiers et les informations (inodes) « stat_data » sont souvent enregistrées les unes à côté des autres. Elles peuvent être lues en une seule opération d'E/S sur disque, ce qui signifie qu'un seul accès au disque suffit pour récupérer toutes les informations nécessaires.

Restauration rapide après une panne
: Le fait d'utiliser un fichier journal pour garder la trace de changements récents de métadonnées ramène la vérification d'un système de fichiers à quelques secondes, même pour de très gros systèmes de fichiers.

Fiabilité via journalisation des données
: ReiserFS prend également en charge la journalisation des données et les modes de données de la même façon que les concepts traités dans la Section 34.2.3, « Ext3 » (p. 553). Le mode par défaut est `data=ordered` qui assure l'intégrité des données et des métadonnées à la fois, mais n'utilise la journalisation que pour les métadonnées.

34.2.2 Ext2

Les origines d'Ext2 remontent au début de l'histoire de Linux. Son prédécesseur, l'Extended File System, a été mis en œuvre en avril 1992 et intégré à Linux 0.96c. L'Extended File System a subi un certain nombre de modifications, pour devenir pendant des années le système de fichiers le plus connu sous Linux sous le nom d'Ext2. Avec l'avènement des systèmes de fichiers journalisés et leurs temps de restauration étonnamment courts, Ext2 a perdu de son importance.

Un bref résumé des points forts d'Ext2 pourrait faire comprendre pourquoi il a été — et dans une certaine mesure est encore — le système de fichiers sous Linux favori de nombreux utilisateurs de ce système d'exploitation.

Stabilité

Étant véritablement un « vénérable vieillard », Ext2 a subi de nombreuses améliorations et a fait l'objet de tests très complets. Cela peut expliquer pourquoi le public le considère souvent « solide comme un roc ». Après une panne de système, quand le système de fichiers ne peut pas être démonté proprement, e2fsck commence à analyser les données du système de fichiers. Les métadonnées sont remises dans un état cohérent, les fichiers ou les blocs de données en attente sont écrits dans un répertoire prévu à cet effet (nommé `lost+found`). Contrairement aux systèmes de fichiers journalisés, e2fsck analyse le système de fichiers entier et non simplement les fragments de métadonnées qui viennent d'être modifiés. L'opération prend sensiblement plus de temps que la vérification d'un système de fichiers journalisé. Selon la taille du système de fichiers, cette procédure peut prendre une demi-heure, voire plus. Par conséquent, il n'est pas souhaitable de choisir Ext2 pour un serveur qui a besoin d'être toujours disponible. Toutefois, puisque Ext2 ne tient pas de journal à jour et utilise sensiblement moins de mémoire, il est parfois plus rapide que d'autres systèmes de fichiers.

Mise à niveau aisée

Le code d'Ext2 constitue la base solide qui a permis à Ext3 de devenir un système de fichiers de nouvelle génération très apprécié. Sa fiabilité et sa stabilité ont été habilement combinées avec les avantages d'un système de fichiers journalisé.

34.2.3 Ext3

Ext3 a été conçu par Stephen Tweedie. Contrairement à tous les autres systèmes de fichiers de nouvelle génération, Ext3 ne suit pas un principe de conception complètement nouveau. Il est basé sur Ext2. Ces deux systèmes de fichiers sont très intimement liés entre eux. Un système de fichiers Ext3 peut très facilement être construitpar-dessus un système de fichiers Ext2. La plus grande différence entre Ext2 et Ext3 est qu'Ext3 permet la journalisation. En résumé, Ext3 offre trois avantages majeurs :

Mises à niveau aisées et extrêmement fiables à partir d'Ext2
Comme Ext3 est basé sur le code d'Ext2 et partage son format de disque ainsi que son format de métadonnées, les mises à niveau d'Ext2 vers Ext3 sont extrêmement faciles. Contrairement aux transitions vers d'autres systèmes de fichiers journalisés, tels que ReiserFS, JFS ou XFS, qui peuvent être assez fastidieuses (faires des sauvegardes du système de fichiers entier et le recréer à partir de zéro), une transition vers Ext3 n'est qu'une question de minutes. Elle est également très sûre, car recréer un système de fichiers entier à partir de zéro pourrait ne pas fonctionner parfaitement. Si l'on considère le nombre de systèmes Ext2 existants qui sont dans l'attente d'une mise à niveau vers un système de fichiers journalisé, vous pouvez aisément comprendre pourquoi Ext3 pourrait être important pour de nombreux administrateurs système. Rétrograder Ext3 en Ext2 est tout aussi facile que de mettre à niveau Ext2 en Ext3. Il suffit de démonter proprement le système de fichiers Ext3 et de le remonter en tant que système de fichiers Ext2.

Fiabilité et performance
D'autres systèmes de fichiers journalisés suivent la méthode qui consiste à journaliser les « métadonnées seulement ». Cela signifie que vos métadonnées sont toujours maintenues dans un état cohérent, mais que la même chose ne peut pas être automatiquement garantie pour les données du système de fichiers elles-mêmes. Ext3 est conçu pour prendre soin à la fois des métadonnées et des données. Le degré d'« attention » peut être adapté à vos préférences personnelles. Le fait d'activer Ext3 dans le mode `data=journal` offre une sécurité maximale (intégrité des données), mais peut ralentir le système car les métadonnées ainsi que les données sont consignées dans le fichier journal. Une approche relativement nouvelle consiste à utiliser le mode `data=ordered`, qui garantit à la fois l'intégrité des données et des métadonnées, mais qui n'utilise la journalisation que pour les métadonnées. Le pilote du système de fichiers rassemble tous les blocs de données qui correspondent à une mise à jour de métadonnées. Ces blocs de données écrits sur le disque avant que les métadonnées ne soient mises à jour. En conséquence, la cohérence est obtenue

pour les métadonnées et les données, sans sacrifier la performance. Une troisième option à utiliser est `data=writeback`, qui permet d'écrire des données dans le système de fichiers principal, une fois ses métadonnées validées dans le fichier journal. Cette option est souvent considérée comme la meilleure en termes de performance. Elle peut cependant permettre à d'anciennes données de réapparaître dans des fichiers après une panne et une restauration, alors que la cohérence interne du système de fichiers interne est conservée. À moins que vous n'ayez spécifié une autre option, Ext3 est lancé avec le paramètre par défaut `data=ordered`.

34.2.4 Convertir un système de fichiers Ext2 en Ext3

La conversion d'un système de fichiers Ext2 en Ext3 comprend deux étapes séparées :

Créer le fichier journal

Connectez-vous en tant que `root` et lancez `tune2fs -j`. Cette commande crée un journal Ext3 avec les paramètres par défaut. Pour décider vous-même de la taille qu'il devra avoir et sur quel disque il devra résider, lancez `tune2fs -J` à la place, avec les options de journal souhaitées `size=` et `device=`. D'autres informations sur le programme tune2fs se trouvent dans sa page de manuel, (tune2fs(8)).

Préciser le type de système de fichiers dans /etc/fstab

Pour vous assurer que le système de fichiers Ext3 est reconnu en tant que tel, ouvrez le fichier `/etc/fstab` et modifiez le type de système de fichiers indiqué pour la partition correspondante, de `ext2` en `ext3`. Le changement entre en vigueur au prochain réamorçage.

Utiliser Ext3 pour le répertoire racine

Pour amorcer un système de fichiers racine configuré en tant que partition Ext3, intégrez les modules `ext3` et `jbd` dans le `initrd`. Pour ce faire, modifiez le fichier `/etc/sysconfig/kernel` pour insérer les deux modules dans la ligne `INITRD_MODULES`, puis exécutez la commande `mkinitrd`.

34.2.5 Reiser4

Juste après la sortie du noyau 2.6, un nouveau membre a rejoint la famille des système de journalisation : Reiser4. Reiser4 est complètement différent de son prédecesseur

ReiserFS (version 3.6). Il introduit le concept de plugins pour mettre au point les fonctionnalités du système de fichiers et un concept de sécurité à granularité plus fine.

Concept de sécurité à granularité fine

Lors de la conception de Reiser4, ses développeurs ont mis l'accent sur l'implémentation des fonctionnalités liées à la sécurité. Reiser4 contient donc un jeu de plugins spécialisés dans la sécurité. Le plus important introduit le concept d'« éléments » de fichier. À l'heure actuelle, les contrôles d'accès aux fichiers sont définis par fichier. Si un grand fichier contient des informations concernant plusieurs utilisateurs, groupes ou applications, les droits d'accès doivent être particulièrement imprécis pour inclure toutes les parties impliquées. Avec Reiser4, vous pouvez diviser ces fichiers en portions plus petites (les « éléments »). Les droits d'accès peuvent alors être attribués séparément pour chaque utilisateur permettant une gestion plus précise de la sécurité des fichiers. `/etc/passwd` en est un exemple parfait. Actuellement, seul `root` peut lire et modifier le fichier tandis que les autres utilisateurs que `root` n'ont qu'un accès en lecture à ce fichier. En utilisant le concept d'éléments de Reiser4, vous pouvez diviser le fichier en un jeu d'éléments (un élément par utilisateur) et permettre aux utilisateurs ou applications de modifier leurs propres données sans accéder aux données des autres utilisateurs. Ce concept permet une plus grande sécurité et une plus grande flexibilité à la fois.

Extensibilité avec les plugins

De nombreuses fonctions de système de fichiers et de fonctions externes utilisés normalement par un système de fichiers sont implémentées en tant que plugins dans Reiser4. Ces plugins peuvent être facilement ajoutés au système de base. Il n'est plus nécessaire de recompiler le noyau ou de reformater le disque dur pour ajouter des nouvelles fonctionnalités à votre système de fichiers.

Meilleure structure du système de fichiers grâce à l'affectation différée

Comme XFS, Reiser4 prend en charge l'affectation différée. Voir la Section 34.2.7, « XFS » (p. 556). L'utilisation de l'affectation différée même pour les métadonnées peut résulter en une meilleure structure.

34.2.6 JFS

JFS, le *Journaling File System*, a été développé par IBM. La première version bêta du portage de JFS sous Linux a été mis à la disposition de la communauté Linux au cours de l'été 2000. La version 1.0.0 a été publiée en 2001. JFS est conçu pour répondre aux besoins des environnements serveur haut débit où les performances sont le but ultime.

Étant un système de fichiers 64 bits complet, JFS prend en charge à la fois les partitions et les fichiers volumineux, ce qui constitue une autre raison de l'utiliser dans des environnements serveur.

Un examen plus détaillé de JFS montre pourquoi ce système de fichiers pourrait se révéler être un bon choix pour votre serveur Linux :

Journalisation efficace
JFS suit une approche « métadonnées seulement ». Au lieu d'une vérification complète, seuls sont vérifiés les changements de métadonnées générés par une activité récente du système de fichiers, ce qui économise énormément de temps lors de la restauration. Des opérations simultanées nécessitant de multiples enregistrements simultanés dans le fichier journal peuvent être combinées en une validation groupée, réduisant ainsi considérablement les baisses de performances du système de fichiers dues à de nombreuses opérations d'écriture.

Organisation efficace des répertoires
JFS reste fidèle à deux organisations différentes de répertoires. Pour de petits répertoires, il permet d'enregistrer directement le contenu du répertoire dans son inode. Pour des répertoires plus volumineux, il utilise des arbres B^+, qui facilitent considérablement la gestion des répertoires.

Meilleure gestion de l'espace grâce à l'allocation dynamique des inodes
Avec Ext2, vous devez définir la densité des inodes à l'avance (l'espace occupé par les informations de gestion), ce qui restreint le nombre maximal de fichiers ou de répertoires de votre système de fichiers. JFS vous évite ces préoccupations—il alloue dynamiquement l'espace des inodes et le libère quand il n'est plus nécessaire.

34.2.7 XFS

Conçu à l'origine conçu comme le système de fichiers pour son système d'exploitation IRIX, SGI a démarré le développement de XFS au début des années 1990. L'idée derrière XFS était de créer un système de fichiers journalisé 64 bits très performant pour répondre aux défis actuels en matière d'informatique extrême. XFS est un très bon outil pour le maniement de fichiers volumineux et se comporte très bien sur du matériel de pointe. Toutefois, XFS présente un inconvénient. Comme ReiserFS, XFS accorde une grande attention à l'intégrité des métadonnées, mais moins à celle des données.

Un rapide examen des fonctionnalités clés de XFS explique pourquoi il pourrait s'avérer un concurrent de poids pour d'autres système de fichiers journalisés dans l'informatique à hautes performances.

Grande capacité à monter en charge grâce à l'utilisation de groupes d'allocation

Au moment de la création d'un système de fichiers XFS, le périphérique bloc à la base du système de fichiers est divisé en huit régions linéaires, voire plus, de taille égale. Ceux-ci sont appelés *groupes d'allocation*. Chaque groupe d'allocation gère ses propres inodes et l'espace disque libre. En pratique, on peut considérer les groupes d'allocation comme des systèmes de fichiers dans un système de fichiers. Comme les groupes d'allocation sont plutôt indépendants les uns par rapport aux autres, plusieurs d'entre eux peuvent être traités simultanément par le noyau. Cette fonctionnalité est la clé de l'excellente capacité à monter en charge de XFS. Naturellement, le principe de groupes d'allocation indépendants convient aux exigences des systèmes multiprocesseurs.

Performances élevées grâce à une gestion efficace de l'espace disque

L'espace libre et les inodes sont gérés par les arbres B^+ à l'intérieur des groupes d'allocation. Le fait d'utiliser des arbres B^+ contribue considérablement aux performances et à la capacité de montée en charge de XFS. XFS utilise l'*affectation différée*. XFS gère l'affectation en divisant le processus en deux. Une transaction en attente est stockée dans la mémoire vive et le volume approprié d'espace est réservé. XFS ne décide pas encore de l'endroit exact (c'est-à-dire les blocs du système de fichiers) où les données devront être stockées. Cette décision est repoussée jusqu'au dernier moment possible. Certaines données temporaires ayant une durée de vie courte peuvent ne jamais être enregistrées sur le disque, car elles risquent d'être obsolètes au moment où XFS décide de l'endroit où les enregistrer. Ainsi, XFS augmente les performances en écriture et réduit la fragmentation du système de fichiers. Comme l'allocation différée entraîne des événements d'écriture moins fréquents que dans d'autres systèmes de fichiers, il est probable que la perte de données après une panne survenant au cours d'un processus d'écriture soit plus grave.

Préallocation pour éviter la fragmentation du système de fichiers

Avant d'écrire les données sur le système de fichiers, XFS *réserve* (préalloue) l'espace libre nécessaire pour un fichier. La fragmentation du système de fichiers est ainsi considérablement réduite. Les performances sont améliorées, car le contenu d'un fichier n'est pas réparti sur la totalité du système de fichiers.

34.3 Autres systèmes de fichiers pris en charge

Le Tableau 34.1, « Types de systèmes de fichiers sous Linux » (p. 558) résume quelques autres système de fichiers pris en charge par Linux. Ils le sont principalement pour assurer la compatibilité et l'échange de données avec différentes sortes de supports ou des systèmes d'exploitation différents.

***Tableau 34.1** Types de systèmes de fichiers sous Linux*

`cramfs`	*Compressed ROM file system* : un système de fichiers compressé en lecture seule pour les mémoires mortes (ROM).
`hpfs`	*High Performance File System* : le système de fichiers standard IBM OS/2 — uniquement pris en charge en mode lecture seule.
`iso9660`	Système de fichiers standard des CD-ROM.
`minix`	Ce système de fichiers est issu de projets universitaires sur les systèmes d'exploitation et est le premier système d'exploitation utilisé sous Linux. Aujourd'hui, il sert de système de fichiers pour les disquettes.
`msdos`	*fat*, le système de fichiers employé à l'origine par DOS, est aujourd'hui utilisé par divers systèmes d'exploitation.
`ncpfs`	Système de fichiers utilisé pour monter des volumes Novell en réseau.
`nfs`	*Network File System* : ici, les données peuvent être enregistrées sur n'importe quelle machine d'un réseau et on y accédera en réseau.
`smbfs`	*Server Message Block* est utilisé par des produits tels que Windows pour permettre l'accès en réseau aux fichiers.
`sysv`	Utilisés sous SCO UNIX, Xenix et Coherent (des systèmes UNIX commerciaux pour PC).

`ufs`	Utilisé par BSD, SunOS et NeXTstep. Pris en charge uniquement en mode lecture seule.
`umsdos`	*UNIX on MSDOS* : appliqué en plus d'un système de fichiers `fat` normal, permet d'obtenir les fonctionnalités offertes par UNIX (droits d'accès, liens, noms de fichiers longs) grâce à la création de fichiers spéciaux.
`vfat`	*Virtual FAT* : extension du système de fichiers `fat` (prend en charge les noms de fichiers longs).
`ntfs`	*Windows NT file system*, lecture seule.

34.4 Prise en charge des fichiers volumineux sous Linux

À l'origine, Linux prenait en charge une taille maximale de fichier de 2 Go. C'était suffisant avant l'explosion du multimédia et tant que personne n'essayait de manipuler d'énormes bases de données sous Linux. Devenant de plus en plus importants pour l'informatique serveur,le noyau et la bibliothèque C ont été modifiés de façon à prendre en charge des tailles de fichiers supérieures à 2 Go grâce à un nouvel ensemble d'interfaces que les applications doivent utiliser. Aujourd'hui, pratiquement tous les systèmes de fichiers les plus importants permettent d'utiliser LFS, ce qui ouvre une porte vers l'informatique à hautes performances. Le Tableau 34.2, « Tailles maximales des systèmes de fichiers (format sur disque) » (p. 559) propose un survol des limitations actuelles des fichiers et systèmes de fichiers sous Linux.

***Tableau 34.2** Tailles maximales des systèmes de fichiers (format sur disque)*

Système de fichiers	Taille du fichier (octets)	Taille du système de fichiers (octets)
Ext2 ou Ext3 (blocs d'une taille de 1 ko)	2^{34} (16 Go)	2^{41} (2 To)

Système de fichiers	Taille du fichier (octets)	Taille du système de fichiers (octets)
Ext2 ou Ext3 (blocs d'une taille de 2 ko)	2^{38} (256 Go)	2^{43} (8 To)
Ext2 ou Ext3 (blocs d'une taille de 4 ko)	2^{41} (2 To)	2^{44} (16 To)
Ext2 ou Ext3 (blocs d'une taille de 8 ko) (systèmes ayant des pages de 8 ko, comme Alpha)	2^{46} (64 To)	2^{45} (32 To)
ReiserFS v3	2^{46} (64 Go)	2^{45} (32 To)
XFS	2^{63} (8 Eo)	2^{63} (8 Eo)
JFS (blocs d'une taille de 512 octets)	2^{63} (8 Eo)	2^{49} (512 To)
JFS (blocs d'une taille de 4 ko)	2^{63} (8 Eo)	2^{52} (4 Po)
NFSv2 (côté client)	2^{31} (2 Go)	2^{63} (8 Eo)
NFSv3 (côté client)	2^{63} (8 Eo)	2^{63} (8 Eo)

IMPORTANT: Limitations du noyau Linux

Le Tableau 34.2, « Tailles maximales des systèmes de fichiers (format sur disque) » (p. 559) décrit les limitations concernant le format de disque. Le noyau 2.6 impose ses propres limites de la taille des fichiers et des systèmes de fichiers qu'il gère :

Taille de fichier

Sur les systèmes 32 bits, les fichiers ne peuvent pas dépasser la taille de 2 To (2^{41} octets).

Taille du système de fichiers

Les systèmes de fichiers peuvent atteindre une taille jusqu'à 2^{73} octets). Cependant, cette limite est encore hors de portée du matériel sur le marché.

34.5 Pour plus d'informations

Chacun des projets de systèmes de fichiers décrit ci-dessus possède son propre site web sur lequel vous trouverez des informations extraites de listes de discussion, de la documentation additionnelle et des FAQ.

- http://e2fsprogs.sourceforge.net/
- http://www.zipworld.com.au/~akpm/linux/ext3/
- http://www.namesys.com/
- http://oss.software.ibm.com/developerworks/opensource/jfs/
- http://oss.sgi.com/projects/xfs/

Un tutoriel complet en plusieurs parties sur les systèmes de fichiers Linux est présent sur le site *IBM developerWorks* à l'adresse suivante : http://www-106.ibm.com/developerworks/library/l-fs.html. Une comparaison des différents systèmes de fichiers journalisés sous Linux réalisée par Juan I. Santos Florido pour la *Linux Gazette* est disponible à l'adresse suivante : http://www.linuxgazette.com/issue55/florido.html. Les personnes intéressées par une analyse approfondie de LFS sous Linux peuvent consulter le site sur LFS d'Andreas Jaeger à l'adresse suivante : http://www.suse.de/~aj/linux_lfs.html.

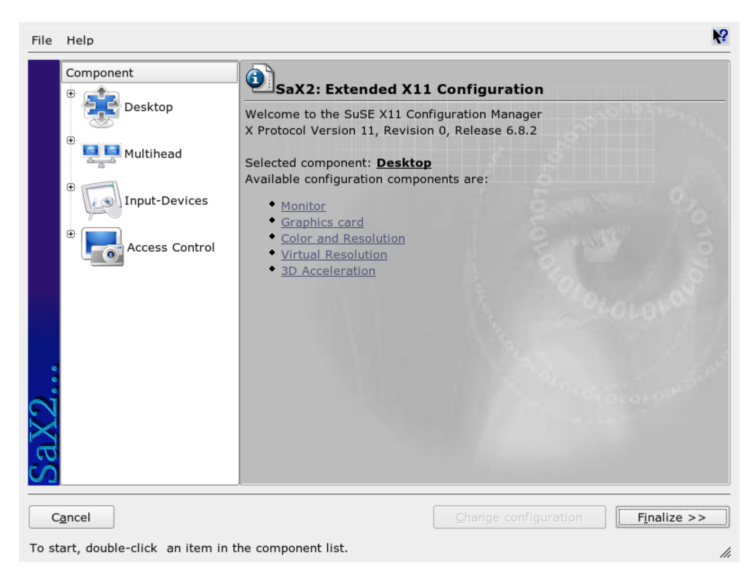
Système X Window 35

Le système X Window (X11) est le standard de fait pour les interfaces graphiques sous UNIX. X est orienté réseau : des applications démarrées sur un hôte peuvent s'afficher sur un autre hôte lorsque les deux ordinateurs sont connectés, quel que soit le type de réseau (LAN ou Internet). Ce chapitre décrit la configuration et l'optimisation de l'environnement système X Window, donne des informations générales sur l'utilisation des polices sous SUSE Linux et explique la configuration des interfaces OpenGL et 3D.

35.1 Configuration de X11 avec SaX2

L'interface utilisateur graphique (serveur X) gère les communications entre le matériel et les logiciels. Les systèmes de bureau, comme KDE et GNOME, ainsi que la plupart des gestionnaires de fenêtres, utilisent le serveur X pour les interactions avec l'utilisateur. L'interface utilisateur graphique est initialement configurée lors de l'installation. Par la suite, pour modifier les paramètres, utilisez le module correspondant du centre de contrôle YaST ou exécutez manuellement SaX2 à partir de la ligne de commande en tapant `sax2`. La fenêtre principale de SaX2 permet d'accéder aux différents modules du centre de contrôle YaST.


Figure 35.1 *Fenêtre principale de SaX2*



La barre de navigation, à gauche, présente six options, qui permettent d'ouvrir chacune la boîte de dialogue de configuration correspondante dans le centre de contrôle YaST. Pour lire les sections mentionnées ci-dessous, consultez le Chapitre *Configuration du système avec YaST* (↑Démarrage).

Moniteur
Pour obtenir une description de la configuration du moniteur et de la carte graphique, consultez la Section « Propriétés des cartes et des moniteurs » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

Souris
Pour obtenir une description de la configuration de la souris dans l'environnement graphique, consultez la Section « Propriétés de la souris » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

Clavier
Pour obtenir une description de la configuration du clavier dans l'environnement graphique, consultez la Section « Propriétés du clavier » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

Tablette
Pour obtenir une description de la configuration de la tablette graphique, consultez la Section « Propriétés de tablette graphique » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

Écran tactile
Pour obtenir une description de la configuration de l'écran tactile, consultez la Section « Propriétés des écrans tactiles » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

VNC
Pour obtenir une description de la configuration de VNC, consultez la Section « Propriétés d'accès distant » (Chapitre 3, *Configuration du système avec YaST*, ↑Démarrage).

35.2 Optimisation de la configuration X

X.Org est une implémentation Open Source du système X Window. Elle a été développée par X.Org Foundation, qui est également responsable du développement de nouvelles technologies et normes pour le système X Window.

La configuration peut être optimisée manuellement pour tirer le meilleur parti de l'équipement disponible, comme la souris, la carte graphique, le moniteur et le clavier. Nous présentons ici quelques aspects de la procédure d'optimisation. Pour plus d'informations sur la configuration du système X Window, consultez les différents fichiers du répertoire `/usr/share/doc/packages/Xorg` ou la page de manuel `man xorg.conf`.

AVERTISSEMENT

Soyez prudent lorsque vous configurez votre système X Window. Ne démarrez jamais le système X Window avant d'avoir terminé la configuration. Un système mal configuré peut endommager votre équipement de manière irréversible (en particulier les moniteurs à fréquence fixe). Les auteurs de ce manuel et SUSE Linux déclinent toute responsabilité concernant les dommages éventuels. Ce texte a été établi avec le plus grand soin ; toutefois, nous ne pouvons pas

garantir que toutes les méthodes présentées ici sont correctes et qu'elles ne présentent pas de risque pour votre équipement.

Les programmes SaX2 et xorgconfig créent le fichier `xorg.conf`, placé par défaut dans le répertoire `/etc/X11`. Il s'agit du fichier de configuration primaire du système X Window. Vous y trouverez les différents paramètres se rapportant à la carte graphique, à la souris et au moniteur.

Les paragraphes suivants décrivent la structure du fichier de configuration `/etc/X11/xorg.conf`. Il est composé de plusieurs sections qui se rapportent chacune à un aspect donné de la configuration. Chaque section est introduite par le mot-clé `Section <désignation>` et se termine par `EndSection`. Ces sections ont le format suivant :

```
Section designation
  entry 1
  entry 2
  entry n
EndSection
```

Les types de sections disponibles sont présentés dans le Tableau 35.1, « Sections dans /etc/X11/xorg.conf » (p. 566).

Tableau 35.1 *Sections dans /etc/X11/xorg.conf*

Type	Signification
`Files`	Cette section décrit les chemins utilisés pour les polices et la table de couleurs RVB.
`ServerFlags`	Les paramètres généraux sont définis ici.
`InputDevice`	Les périphériques d'entrée, comme les claviers et les équipements spéciaux (pavés tactiles, joysticks, etc.), sont configurés dans cette section. Ici, les paramètres importants sont `Driver` (Pilote), ainsi que les options qui permettent de définir le protocole (`Protocol`) et le périphérique (`Device`).
`Moniteur`	Cette section décrit le moniteur utilisé. Les éléments de cette section sont le nom, auquel la définition `Screen` (écran) fait ensuite référence, la bande passante (`Bandwidth`) et les limites de fréquence de synchronisation (`HorizSync` et

Type	Signification
	VertRefresh). Les valeurs sont indiquées en MHz, en kHz ou en Hz. En principe, le serveur refuse les valeurs modeline qui ne correspondent pas à la fréquence du moniteur. Cela évite d'indiquer par mégarde au moniteur des fréquences trop élevées.
Modes	C'est ici que sont stockés les paramètres modeline représentatifs de chaque résolution d'écran. Ces paramètres peuvent être calculés par SaX2 sur la base des valeurs indiquées par l'utilisateur et n'ont en principe pas besoin d'être modifiés Vous pouvez toutefois intervenir manuellement, notamment si vous souhaitez vous connecter à un moniteur à fréquence fixe. Vous trouverez des informations plus détaillées sur la signification des différentes valeurs numériques dans le fichier HOWTO (Guide pratique) /usr/share/doc/howto/en/ XFree86-Video-Timings-HOWTO.gz.
Device	Cette section définit une carte graphique spécifique. Elle est référencée à l'aide de son nom descriptif.
Screen	Cette section associe un moniteur (Monitor) et un périphérique (Device) pour former tous les paramètres nécessaires pour X.Org. La sous-section Display permet de spécifier la taille de l'écran virtuel (Virtual), la fenêtre d'affichage (ViewPort) et les modes utilisés avec cet écran.
ServerLayout	Cette section définit la structure d'une configuration single ou multihead. Cette section lie également les périphériques d'entrée (InputDevice) et ceux d'affichage (Screen).

Les sections Monitor, Device et Screen sont décrites en détail ci-après. Vous trouverez des informations sur les autres sections dans les pages de manuel associées à X.Org et à xorg.conf.

Il peut y avoir plusieurs sections Monitor et Device dans le fichier xorg.conf. Vous pouvez même y trouver plusieurs sections Screen. La section ServerLayout qui suit détermine les éléments utilisés.

35.2.1 Section Screen

Commencez par observer en détail la section Screen, qui associe une section Monitor et une section Device, et détermine la résolution et la profondeur de couleurs à utiliser. Une section Screen peut se présenter comme dans l'Exemple 35.1, « Section Screen du fichier /etc/X11/xorg.conf » (p. 568).

***Exemple 35.1** Section Screen du fichier /etc/X11/xorg.conf*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

La ligne `Identifier` (ici, `Screen[0]`) attribue à cette section un nom spécifique qui permet de la référencer de façon unique dans la section `ServerLayout` qui suit. Les lignes `Device` et `Monitor` spécifient la carte graphique et le moniteur qui appartiennent à cette définition. Il s'agit simplement de liens vers les sections `Device` et `Monitor`, avec leurs noms ou leurs *identificateurs* propres. Ces sections sont décrites plus loin.

Le paramètre `DefaultDepth` permet de sélectionner la profondeur de couleurs que le serveur doit utiliser, sauf s'il est démarré avec une profondeur de couleurs spécifique. À chaque profondeur de couleurs correspond une sous-section `Display`. Le mot-clé `Depth` fixe la profondeur de couleurs valide pour cette sous-section. Les valeurs admises

pour Depth sont 8, 15, 16 et 24. Certains modules serveur X n'admettent pas forcément toutes ces valeurs.

Après la profondeur de couleurs, vous établissez une liste de résolutions dans la section Modes. Le serveur X consulte cette liste de gauche à droite. Pour chaque résolution, le serveur X recherche une valeur modeline adéquate dans la section Modes. La valeur modeline dépend à la fois des capacités du moniteur et de celles de la carte graphique. Les paramètres de la section Monitor déterminent la valeur modeline résultante.

La première résolution trouvée est le mode par défaut (Default mode). La combinaison de touches Ctrl + Alt + + (pavé numérique) permet de se déplacer dans la liste des résolutions, de gauche à droite. La combinaison de touches Ctrl + Alt + – (pavé numérique) permet de se déplacer vers la gauche. Vous pouvez ainsi changer de résolution pendant que X est en cours d'exécution.

La dernière ligne de la sous-section Display, avec Depth 16, se rapporte à la taille de l'écran virtuel. La taille maximum d'un écran virtuel dépend de la quantité de mémoire installée sur la carte graphique et de la profondeur de couleurs souhaitée ; la résolution maximum du moniteur n'a aucun impact. Comme les cartes graphiques modernes ont une mémoire vidéo grande capacité, elles permettent de créer des bureaux virtuels de grande taille. Toutefois, vous risquez de ne plus pouvoir utiliser les fonctionnalités 3D si vous surchargez la mémoire vidéo avec un bureau virtuel trop étendu. Si la carte dispose de 16 Mo de RAM vidéo, par exemple, l'écran virtuel peut avoir une taille maximum de 4 096 x 4 096 pixels avec une profondeur de couleurs de 8 bits. Il est cependant recommandé, en particulier pour les cartes accélérées, de ne pas consacrer l'intégralité de la mémoire à l'écran virtuel, car cette mémoire intégrée à la carte sert également à plusieurs polices et caches graphiques.

35.2.2 Section Device

Une section Device décrit une carte graphique spécifique. Vous pouvez créer dans le fichier xorg.conf autant d'entrées Device que vous le souhaitez, à condition de différencier leur noms à l'aide du mot-clé Identifier. En principe, si vous avez installé plusieurs cartes graphiques, les sections sont simplement numérotées de façon séquentielle. La première section est appelée Device[0], la deuxième Device[1], etc. Le fichier ci-dessous présente un extrait de la section Device d'un ordinateur équipé d'une carte graphique PCI Matrox Millennium :

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Si vous utilisez SaX2 pour la configuration, la section Device devrait ressembler à l'exemple ci-dessus. Les deux paramètres `Driver` et `BusID`, qui dépendent du matériel installé sur l'ordinateur, sont détectés automatiquement par SaX2. Le paramètre `BusID` détermine l'emplacement PCI ou AGP où la carte graphique est installée. Cette valeur correspond à l'ID affiché par la commande lspci. Le serveur X utilise la notation décimale mais la commande lspci affiche les valeurs au format hexadécimal.

Le paramètre `Driver` permet de spécifier le pilote à utiliser pour cette carte graphique. Dans le cas d'une carte Matrox Millennium, le module pilote s'appelle `mga`. Le serveur X examine alors le chemin `ModulePath` défini dans la section `Files` jusqu'au sous-répertoire `drivers`. Dans une installation standard, il s'agit du répertoire `/usr/X11R6/lib/modules/drivers`. Le suffixe `_drv.o` est ajouté au nom. Ainsi, pour le pilote `mga`, le système charge le fichier de pilote `mga_drv.o`.

Des options supplémentaires permettent d'influencer le comportement du serveur X ou du pilote. C'est le cas, notamment, de l'option `sw_cursor`, définie dans la section Device. Cette option désactive le curseur matériel de la souris et le trace par voie logicielle. Suivant le module de pilote utilisé, diverses options sont disponibles, que vous pouvez consulter dans les fichiers de description des modules de pilote dans le répertoire `/usr/X11R6/lib/X11/doc`. En principe, les options valides sont également décrites dans les pages de manuel (`man xorg.conf` et `man X.Org`).

35.2.3 Sections Monitor et Modes

Comme les sections `Device`, les sections `Monitor` et `Modes` décrivent chacune un moniteur. Le fichier de configuration `/etc/X11/xorg.conf` peut contenir autant de sections `Monitor` que vous le souhaitez. La section ServerLayout permet de spécifier ensuite la section `Monitor` à appliquer.

Les définitions de moniteur ne doivent être configurées que par des utilisateurs confirmés. Les valeurs modeline forment une partie importante des sections `Monitor`. Les valeurs modeline définissent les fréquences de synchronisation horizontale et verticale

associées à chaque résolution. Les propriétés du moniteur, notamment les fréquences admises, sont stockées dans la section `Monitor`.

AVERTISSEMENT

Il est conseillé de ne pas modifier les valeurs modeline sans connaissance approfondie des fonctions du moniteur et de la carte graphique, car vous risquez d'endommager gravement le moniteur.

Les utilisateurs suffisamment expérimentés pour développer leurs propres configurations de moniteur doivent avoir soigneusement consulté la documentation du répertoire `/usr/X11/lib/X11/doc`. La section qui traite des modes vidéo offre un intérêt tout particulier. Elle décrit en détail le mode de fonctionnement du matériel et la procédure à suivre pour créer des valeurs modeline.

Actuellement, il est rarement nécessaire de définir manuellement les valeurs modeline. En principe, si vous utilisez un moniteur MultiSync moderne, les fréquences admises et les résolutions optimales sont lues directement par le serveur X via DDC, comme le décrit la section qui présente la configuration de SaX2. Si cela n'est pas possible pour une raison quelconque, utilisez l'un des modes VESA intégrés au serveur X. Cela devrait fonctionner sans problèmes sur presque toutes les combinaisons carte graphique/moniteur.

35.3 Installation et configuration de polices

L'installation de polices supplémentaires sous SUSE Linux est une opération très simple. Il suffit de copier les polices vers un répertoire situé sur le chemin des polices X11 (consultez la Section 35.3.2, « Polices X11 de base » (p. 576)). Pour que les polices puissent être appliquées, leur répertoire d'installation doit être un sous-répertoire des répertoires configurés dans le fichier `/etc/fonts/fonts.conf` (consultez la Section 35.3.1, « Xft » (p. 572)).

Vous pouvez copier les fichiers manuellement (en tant qu'utilisateur `root`) vers un répertoire approprié, comme `/usr/X11R6/lib/X11/fonts/truetype`. Vous pouvez aussi utiliser le programme d'installation de polices KDE, qui se trouve dans le centre de contrôle KDE. Le résultat est identique.

Bien entendu, au lieu de copier les polices proprement dites, vous pouvez créer des liens symboliques. Cela peut être utile, par exemple, si vous avez des polices sous licence dans une partition Windows montée et que vous souhaitez les utiliser. Vous devez exécuter ensuite la commande `SuSEconfig --module fonts` .

La commande `SuSEconfig --module fonts` exécute le script `/usr/sbin/fonts-config`, qui gère la configuration des polices. Pour plus de détails sur ce script et ses effets, consultez la page de manuel correspondante (`man fonts-config`).

La procédure est identique pour tous les types de polices : bitmaps, TrueType, OpenType ou Type1 (PostScript). Tous ces types de polices peuvent être installés le répertoire de votre choix. Seules les polices codées en CID exigent une procédure légèrement différente. Pour plus d'informations, consultez la Section 35.3.3, « Polices codées en CID » (p. 577).

X.Org regroupe deux systèmes de polices complètement différents : l'ancien *système de polices X11 de base* et le tout nouveau système *Xft et fontconfig*. Les sections suivantes décrivent brièvement ces deux systèmes.

35.3.1 Xft

Dès le départ, les programmeurs qui ont développé Xft ont veillé à ce que le système prenne en charge les polices vectorielles, et en particulier le lissage. Avec Xft, contrairement aux polices X11 de base, c'est l'application qui utilise les polices qui assure le rendu, et non le serveur X. Ainsi, l'application concernée a accès aux fichiers de polices réels et peut contrôler le rendu des caractères (glyphes). Cela permet une représentation correcte des caractères dans de nombreuses langues. L'accès direct aux fichiers de polices est très utile pour incorporer des polices lors de l'impression afin de garantir un résultat fidèle à l'image à l'écran.

Dans SUSE Linux, les deux environnements de bureau KDE et GNOME, Mozilla, ainsi que nombreuses autres applications, utilisent déjà Xft par défaut. Xft est déjà utilisé par bien d'autres applications que l'ancien système de polices X11 de base.

Xft utilise la bibliothèque fontconfig pour rechercher les polices et influer sur leur rendu. Les propriétés de fontconfig sont contrôlées par le fichier de configuration globale (`/etc/fonts/fonts.conf`) et le fichier de configuration propre à

l'utilisateur (~/.fonts.conf). Chacun des fichiers de configuration de fontconfig doit commencer par :

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

et se terminer par :

```
</fontconfig>
```

Pour ajouter des répertoires où rechercher des polices, ajoutez des lignes du type :

```
<dir>/usr/local/share/fonts/</dir>
```

Toutefois, cela est généralement inutile. Par défaut, le répertoire propre à l'utilisateur (~/.fonts) est déjà entré dans /etc/fonts/fonts.conf. Ainsi, pour installer des polices supplémentaires, il suffit de les copier vers ~/.fonts.

Vous pouvez également introduire des règles qui influent sur l'aspect des polices. Par exemple, vous pouvez entrer :

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

afin de désactiver le lissage pour toutes les polices, ou bien

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

pour désactiver le lissage pour des polices spécifiques.

Par défaut, la plupart des applications utilisent les noms de polices sans-serif (ou l'équivalent : sans), serifou monospace. Il ne s'agit pas de polices réelles, mais simplement d'alias qui désignent une police appropriée, en fonction de la langue définie.

Les utilisateurs peuvent ajouter facilement des règles à leur fichier ~/.fonts.conf pour que ces alias pointent vers leurs polices favorites :

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Comme pratiquement toutes les applications utilisent ces alias par défaut, ces règles affectent la quasi-totalité du système. Vous pouvez donc facilement utiliser vos polices favorites presque partout, sans avoir à modifier le paramétrage des polices dans chaque application.

La commande `fc-list` permet de connaître les polices installées et disponibles. La commande `fc-list`, par exemple, renvoie la liste de toutes les polices. Pour connaître, parmi les polices vectorielles disponibles (`:outline=true`), celles qui contiennent tous les caractères hébraïques (`:lang=he`), connaître leurs noms (`family`), leur style (`style`), leur graisse (`weight`) et le nom du fichier où elles sont stockées, entrez la commande suivante :

```
fc-list ":lang=he:outline=true" family style weight
```

La sortie de cette commande peut se présenter comme suit :

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
```

```
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Paramètres importants que vous pouvez rechercher avec `fc-list` :

Tableau 35.2 *Paramètres de fc-list*

Paramètre	Signification et valeurs possibles
`family`	Nom de la famille de polices, comme `FreeSans`.
`foundry`	Nom du créateur de cette police, comme `urw`.
`style`	Style de police : `Medium` (moyen), `Regular` (standard), `Bold` (gras), `Italic` (italique) ou `Heavy` (épais).
`lang`	Langue prise en charge par la police ; par exemple, `de` pour l'allemand, `ja` pour le japonais, `zh-TW` pour le chinois traditionnel ou `zh-CN` pour le chinois simplifié.
`weight`	Graisse de la police : `80` pour une police standard, `200` pour des caractères gras.
`slant`	Inclinaison : généralement, `0` pour une police standard et `100` pour l'italique.
`file`	Nom du fichier contenant la police.
`outline`	`true` s'il s'agit d'une police contour, `false` dans le cas contraire.
`scalable`	`true` s'il s'agit d'une police vectorielle, `false` dans le cas contraire.
`bitmap`	`true` s'il s'agit d'une police bitmap, `false` dans le cas contraire.
`pixelsize`	Taille de police, en pixels. L'utilisation de cette option avec fc-list n'est justifiée que pour les polices bitmaps.

35.3.2 Polices X11 de base

Actuellement, le système de polices X11 de base prend en charge non seulement les polices bitmaps, mais aussi les polices vectorielles (Type1, TrueType et OpenType) et celles codées en CID. Les polices Unicode sont également prise en charge depuis déjà assez longtemps. À l'origine, en 1987, le système de polices X11 de base a été développé pour X11R1 afin de gérer les polices bitmaps monochromes. Toutes les extensions mentionnées plus haut ont été ajoutées par la suite.

Ainsi, les polices vectorielles sont prises en charge uniquement sans lissage ni rendu au niveau des sous-pixels, et le chargement des polices vectorielles de grande taille avec des caractères correspondant à de nombreuses langues peut être très long. L'utilisation des polices Unicode peut aussi s'avérer lente et gourmande en mémoire.

Le système de polices X11 de base présente quelques points faibles. Il a beaucoup vieilli et aucune extension n'est plus vraiment efficace. Bien qu'il doive être conservé pour des raisons de compatibilité avec les versions précédentes, il est conseillé d'utiliser le système Xft et fontconfig, bien plus moderne, si vous le pouvez.

Pour fonctionner, le serveur X doit connaître les polices disponibles et leur emplacement sur le système. Cela est géré par la variable FontPath, qui contient le chemin de tous les répertoires de polices valides du système. Dans chacun de ces répertoires, un fichier nommé `fonts.dir` répertorie les polices disponibles. La variable FontPath est générée par le serveur X au démarrage. Le système recherche un fichier `fonts.dir` valide dans chacune des entrées `FontPath` du fichier de configuration `/etc/X11/xorg.conf`. Ces entrées se trouvent sous la section `Files`. La commande `xset q` permet d'afficher le chemin FontPath réel. Vous pouvez aussi modifier ce chemin pendant l'exécution, avec xset. La commande `xset +fp <chemin>` permet d'ajouter un chemin. Pour supprimer un chemin inutile, utilisez `xset -fp <chemin>`.

Si le serveur X est déjà actif, les polices nouvellement installées dans des répertoires montés peuvent être rendues accessibles via la commande `xset fp rehash`. Cette commande est exécutée par `SuSEconfig --module fonts`. Comme la commande `xset` a besoin d'accéder au serveur X en cours d'exécution, cela ne fonctionne que si `SuSEconfig --module fonts` est lancée à partir d'un shell qui a accès au serveur X actif. La méthode la plus simple consiste à s'identifier comme utilisateur `root` en entrant la commande `su` et le mot de passe approprié. La commande `su` transmet au shell racine (root) les autorisations d'accès de l'utilisateur qui a démarré le serveur X. Pour vérifier si les polices ont été correctement installées et sont disponibles via le système

de polices X11 de base, utilisez la commande `xlsfonts` pour répertorier toutes les polices disponibles.

Par défaut, SUSE Linux utilise les paramètres régionaux UTF-8. Il est donc conseillé d'utiliser des polices Unicode (noms de police qui finissent par `iso10646-1` dans la sortie de la commande `xlsfonts`). Pour dresser la liste de toutes les polices Unicode disponibles, utilisez `xlsfonts | grep iso10646-1`. Pratiquement toutes les polices Unicode disponibles dans SUSE Linux contiennent au moins tous les glyphes nécessaires pour les langues européennes (anciennement codés en `iso-8859-*`).

35.3.3 Polices codées en CID

Contrairement aux autres types de polices, vous ne pouvez pas installer les polices codées en CID n'importe où. Elles doivent être installées dans `/usr/share/ghostscript/Resource/CIDFont`. Cela ne concerne pas le système Xft et fontconfig, mais c'est nécessaire pour Ghostscript et le système de polices X11 de base.

ASTUCE

Pour plus d'informations sur les polices sous X11, consultez le site `http://www.xfree86.org/current/fonts.html`.

35.4 Configuration de OpenGL—3D

35.4.1 Prise en charge du matériel

SUSE Linux comprend divers pilotes OpenGL pour la prise en charge du matériel 3D. Vous trouverez un aperçu dans le Tableau 35.3, « Matériel 3D pris en charge » (p. 577).

Tableau 35.3 *Matériel 3D pris en charge*

Pilote OpenGL	Matériel pris en charge
nVidia	Chipset nVidia : tous sauf Riva 128(ZX)

Pilote OpenGL	Matériel pris en charge
DRI	3Dfx Voodoo Banshee, 3Dfx Voodoo-3/4/5, Intel i810/i815/i830M, Intel 845G/852GM/855GM/865G/915, Matrox G200/G400/G450/G550, ATI Rage 128(Pro)/Radeon (jusqu'à 9250)

Lors d'une première installation avec YaST, l'accélération 3D peut être activée dès l'installation, si YaST offre la prise en charge correspondante. En présence de composants graphiques nVidia, il faut d'abord installer le pilote nVidia. Pour cela, choisissez pendant l'installation le correctif du pilote nVidia dans YOU (YaST Online Update). Nous ne pouvons malheureusement pas vous fournir le pilote nVidia pour des questions de licence.

Si une mise à jour a été installée, la prise en charge du matériel 3D doit être configurée de manière différente. La procédure dépend là du pilote OpenGL à utiliser et est expliquée plus précisément dans la section suivante.

35.4.2 Pilote OpenGL

Ces pilotes OpenGL peuvent être aisément configurés avec SaX2. Notez que pour des cartes nVidia, le pilote nVidia doit être installé au préalable (voir plus haut). Utilisez la commande `3Ddiag` pour vérifier si la configuration de nVidia ou DRI est correcte.

Pour des raisons de sécurité, seuls les utilisateurs du groupe `video` ont accès au matériel 3D. Assurez-vous par conséquent que tous les utilisateurs travaillant localement sur l'ordinateur sont enregistrés dans ce groupe. Sinon, on utilise, pour les programmes OpenGL, le plus lent *Software Rendering Fallback* du pilote OpenGL. Utilisez la commande `id` pour vérifier si l'utilisateur actuel appartient au groupe `video`. Si ce n'est pas le cas, vous pouvez l'ajouter à ce groupe avec YaST.

35.4.3 Outil de diagnostic 3Ddiag

Pour pouvoir vérifier la configuration 3D sous SUSE Linux, vous disposez de l'outil de diagnostic 3Ddiag. Veuillez noter qu'il s'agit d'un outil en ligne de commande que vous devez utiliser dans un terminal. Saisissez `3Ddiag -h` pour afficher les possibles options de 3Ddiag.

Pour vérifier la configuration de X.Org, le programme s'assure que les paquetages nécessaires à la prise en charge 3D sont installés et si la bibliothèque OpenGL ainsi que l'extension GLX correctes sont utilisées. Veuillez suivre les instructions de 3Ddiag quand apparaissent des messages « failed ». En cas de succès, seuls des messages « done » sont affichés à l'écran.

35.4.4 Programmes test pour OpenGL

Outre `glxgears`, des jeux comme `tuxracer` et `armagetron` (paquetage du même nom) conviennent bien comme programmes de test pour OpenGL. Si la prise en charge de la 3D est activée, ils s'affichent de manière fluide sur l'écran d'un ordinateur à peu près actuel. Sans prise en charge de la 3D, ceci est insensé (effet diapositives). L'affichage de `glxinfo` informe précisément de l'état d'activation de la prise en charge de la 3D. Si elle est bien activée, le résultat contiendra la ligne `direct rendering: Yes`.

35.4.5 Dépannage

Si le résultat du test 3D OpenGL s'avère être négatif, (pas de jeu fluide possible), vérifiez d'abord avec 3Ddiag s'il n'existe pas d'erreur de configuration (messages « failed »). Si leur correction ne résout pas le problème, cela ne change rien ou s'il n'y avait aucun message « failed », il suffit souvent de consulter les fichiers Log de X.Org. Ici, on trouve souvent dans `/var/log/Xorg.0.log` de X.Org la ligne `DRI is disabled`. Il peut y avoir plusieurs causes que l'on ne peut cependant trouver qu'en effectuant un examen précis du fichier journal, ce qui souvent dépasse le débutant.

Dans ces cas, il ne s'agit pas en règle générale d'une erreur de configuration puisque celle-ci aurait déjà été détectée par 3Ddiag. Donc, la seule solution encore possible est d'utiliser le Software Rendering Fallback du pilote DRI, qui n'offre cependant aucune prise en charge de la 3D. De même, il vaut mieux renoncer à l'utilisation de la prise en

charge de la 3D quand surviennent des erreurs de représentation OpenGL ou même des problèmes de stabilité. Utilisez SaX2 pour désactiver la prise en charge de la 3D.

35.4.6 Assistance à l'installation

Outre le `Software Rendering Fallback` du pilote DRI, tous les pilotes OpenGL sous Linux sont encore en développement et doivent donc être considérés comme des pilotes expérimentaux. Nous avons cependant pris la décision de fournir les pilotes dans cette distribution, car il y a une grosse demande d'accélération matérielle 3D sous Linux. En raison du stade actuel expérimental des pilotes OpenGL, nous ne pouvons cependant pas étendre le cadre de l'assistance à l'installation à la configuration de l'accélération matérielle 3D et ne pouvons pas vous venir en aide en cas de problèmes s'y rapportant. L'installation de base de l'interface utilisateur graphique X11 ne comprend donc en aucun cas aussi l'installation de l'accélération matérielle 3D. Cependant nous espérons que ce chapitre a déjà répondu à beaucoup de vos questions à ce sujet. Si vous rencontrez des problèmes avec la prise en charge du matériel 3D, nous vous conseillons, en cas de doute, de vous passer de cette prise en charge.

35.4.7 Documentation en ligne additionnelle

Des informations sur DRI sont disponibles dans `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`). Vous trouverez des informations sur l'installation du pilote nvidia sous http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html.

Authentification avec les modules PAM

36

Linux utilise les modules PAM (Pluggable Authentication Modules - modules d'authentification enfichables) au cours de son processus d'authentification comme couche intermédiaire entre l'utilisateur et l'application. Les modules PAM sont disponibles sur l'ensemble du système : n'importe quelle application peut donc les demander. Ce chapitre décrit le mode de fonctionnement de ce mécanisme d'authentification modulaire, ainsi que son mode de configuration.

Il n'est pas rare que les administrateurs système et les programmeurs veuillent restreindre l'accès à certaines parties du système ou limiter l'utilisation de certaines fonctions d'une application. Sans les modules PAM, les applications doivent se réadapter chaque fois qu'un nouveau mécanisme d'authentification (LDAP ou SAMBA, par exemple) est disponible sur le marché. Ce processus, cependant, demande du temps et est source d'erreurs. Aussi, pour éviter ces inconvénients, l'une des solutions est de séparer les applications du mécanisme d'authentification et de déléguer cette authentification à des modules gérés de manière centrale. Chaque fois qu'un programme d'authentification nouvellement requis est nécessaire, il suffit d'adapter ou d'écrire le module PAM approprié utilisé par le programme en question.

Chaque programme fondé sur un mécanisme PAM possède son propre fichier de configuration dans le répertoire `/etc/pam.d/`*`nomduprogramme`*. Ces fichiers définissent les modules PAM utilisés pour l'authentification. De plus, il existe des fichiers de configuration globale pour la plupart des modules PAM dans le répertoire `/etc/security`, qui définissent le comportement exact de ces modules (exemples : `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` et `time.conf`). Chaque application qui utilise un module PAM appelle en fait un ensemble de fonctions PAM. Ces fonctions traitent ensuite les informations des différents fichiers de configuration et renvoient les résultats à l'application appelante.

36.1 Structure d'un fichier de configuration PAM

Chaque ligne d'un fichier de configuration PAM contient quatre colonnes au maximum :

```
<Type of module (Type de module)> <Control flag (drapeau de contrôle)> <Module
 path (Chemin d'accès au module)> <Options>
```

Les modules PAM sont traités comme des piles. Chaque type de module a une utilité différente. Par exemple, un module contrôlera le mot de passe, un deuxième vérifiera l'emplacement à partir duquel l'accès au système est requis et un troisième lira les paramètres personnalisés des utilisateurs. Les types de modules PAM sont au nombre de quatre :

`auth`
: Ce type de module a pour but de vérifier l'authenticité de l'utilisateur. Traditionnellement, cette opération est exécutée via la demande d'un mot de passe, mais elle est également possible avec l'aide d'une carte à puce ou via des informations biométriques (analyse d'empreintes digitales ou de l'iris).

`compte`
: Les modules de ce type contrôlent si l'utilisateur bénéficie d'autorisations générales pour utiliser le service demandé. Exemple : ce type de contrôle peut être exécuté pour garantir que personne ne peut se loguer sous le nom d'utilisateur d'un compte arrivé à expiration.

`password`
: Ce type de module a pour but d'autoriser la modification d'un jeton d'authentification. Dans la plupart des cas, il s'agit d'un mot de passe.

`session`
: Les modules de ce type sont responsables de la gestion et de la configuration des sessions utilisateur. Ils sont lancés avant et après l'authentification pour enregistrer les tentatives de login dans des journaux système et pour configurer l'environnement propre à un utilisateur (comptes de messagerie, répertoire privé, limites système, etc.).

La seconde colonne contient les drapeaux de contrôle pour influencer le comportement des modules lancés :

required
: Un module portant ce drapeau doit être exécuté avec succès pour que l'authentification puisse se poursuivre. En cas d'échec d'un module doté du drapeau `required`, tous les autres modules portant ce même drapeau sont traités et ce n'est qu'après que l'utilisateur reçoit un message l'informant de l'échec de la tentative d'authentification.

requisite
: Les modules portant ce drapeau doivent également être traités avec succès, plus ou moins comme un module doté du drapeau `required`. Par contre, en cas d'échec, l'utilisateur en est immédiatement averti et aucun autre module n'est traité. En cas de réussite, les autres modules sont traités après, comme tout autre module doté du drapeau `required`. Le drapeau `requisite` peut être utilisé comme filtre de base pour vérifier certaines conditions fondamentales pour une authentification correcte.

sufficient
: Après la réussite du traitement d'un module portant ce drapeau, l'application appelante reçoit immédiatement un message lui confirmant cette réussite et aucun autre module n'est traité, à condition qu'il n'y a pas eu précédemment d'échec d'un module doté du drapeau `required`. L'échec d'un module doté du drapeau `sufficient` n'a pas de conséquence directe, dans le sens où les modules ultérieurs sont traités dans leur ordre respectif.

optional
: L'échec ou le succès d'un module portant ce drapeau n'a pas de conséquence directe. Cela peut s'avérer pratique pour les modules dont la seule fonctionnalité est d'afficher un message (par exemple, pour avertir l'utilisateur de l'arrivée d'un message), sans exécuter d'autre action.

include
: Lorsque ce drapeau est attribué, le fichier indiqué en argument est inséré à cet endroit.

Le chemin d'accès au module n'a pas besoin d'être indiqué de manière explicite, du moment que ce module est situé dans le répertoire par défaut `/lib/security` (pour toutes les plates-formes 64 bits prises en charge par SUSE Linux, il s'agit du répertoire `/lib64/security`). La quatrième colonne peut contenir une option pour le module indiqué, telle que `debug` (pour activer le débogage) ou `nullok` (pour autoriser l'utilisation de mots de passe vides).

36.2 Configuration PAM de sshd

Pour illustrer la théorie sous-jacente aux modules PAM et en comprendre les rouages, prenez l'exemple pratique suivant de la configuration PAM de sshd :

***Exemple 36.1** Configuration PAM de sshd*

```
#%PAM-1.0
auth     include        common
auth auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Activez la ligne suivante pour obtenir la prise en charge resmgr pour
# les sessions ssh (reportez-vous à /usr/share/doc/packages/resmgr/README.SUSE)
#session  optional      pam_resmgr.so fake_ttyname
```

La configuration PAM type d'une application (sshd, dans le cas présent) contient quatre instructions include qui font référence aux fichiers de configuration de quatre types de modules : `common-auth`, `common-account`, `common-password` et `common-session`. Ces quatre fichiers détiennent la configuration par défaut de chaque type de module. En incluant ces instructions au lieu d'appeler chaque module séparément pour chaque application PAM, vous obtenez automatiquement la mise à jour d'une configuration PAM si l'administrateur change les paramètres par défaut. Avant, lorsque des modifications étaient apportées aux modules PAM ou qu'une nouvelle application était installée, vous deviez régler tous les fichiers de configuration manuellement pour toutes les applications. Désormais, la configuration PAM s'effectue de façon centralisée via les fichiers de configuration : ainsi, la configuration PAM de chaque périphérique hérite automatiquement du moindre changement.

Le premier fichier include (`common-auth`) appelle deux modules de type `auth` : `pam_env` et `pam_unix2`. (voir Exemple 36.2, « Configuration par défaut de la section `auth` » (p. 584)).

***Exemple 36.2** Configuration par défaut de la section auth*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

Le premier module, `pam_env`, charge le fichier `/etc/security/pam_env.conf` pour définir les variables d'environnement conformément aux spécifications de ce fichier. Cela peut être utilisé pour définir la valeur appropriée pour la variable `DISPLAY`. Le module `pam_env` connaît en effet l'emplacement à partir duquel est exécuté le

login. Le deuxième module, pam_unix2, contrôle le login et le mot de passe de l'utilisateur en fonction des informations des répertoires /etc/passwd et /etc/shadow.

Une fois les modules indiqués dans common-auth appelés avec succès, un troisième module, pam_nologin, vérifie si le fichier /etc/nologin existe. S'il existe, seul l'utilisateur root peut se loguer. La totalité de la pile des modules auth est traitée et ce n'est qu'ensuite que sshd est informé de la réussite ou de l'échec du login. Étant donné que tous les modules de la pile portent le drapeau required, ils doivent tous être traités avec succès pour que sshd puisse recevoir un message lui confirmant la réussite de l'opération. En cas d'échec de l'un des modules, le reste de la pile continue à être traité et ce n'est qu'ensuite que sshd est averti de cet échec.

Dès que tous les modules de type auth ont été traités avec succès, une autre instruction include est traitée (dans le cas présent, voir l'Exemple 36.3, « Configuration par défaut de la section account » (p. 585)). common-account ne contient qu'un seul module, pam_unix2. Si pam_unix2 renvoie un résultat indiquant que l'utilisateur existe, sshd reçoit un message de confirmation et la prochaine pile de modules (password) est traitée, comme dans l'Exemple 36.4, « Configuration par défaut de la section password » (p. 585).

Exemple 36.3 *Configuration par défaut de la section account*

```
account required        pam_unix2.so
```

Exemple 36.4 *Configuration par défaut de la section password*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

Une fois encore, la configuration PAM de sshd implique seulement une instruction include faisant référence à la configuration par défaut des modules password dans common-password. Ces modules doivent être exécutés avec succès (drapeau de contrôle required) chaque fois que l'application requiert qu'un jeton d'authentification soit modifié. Le changement d'un mot de passe ou d'un autre jeton d'authentification requiert un contrôle de sécurité. Cette opération est exécutée à l'aide du module pam_pwcheck. Le module pam_unix2 utilisé ensuite reprend les anciens et nouveaux mots de passe dans pam_pwcheck : l'utilisateur n'a donc pas besoin de s'authentifier à nouveau. Ainsi, il est également impossible d'éviter les contrôles menés par pam_pwcheck. Les modules de type password doivent être utilisés chaque fois que les

modules précédents de type account ou auth sont configurés pour signaler l'arrivée à expiration d'un mot de passe.

Exemple 36.5 *Configuration par défaut de la section session*

```
session required        pam_limits.so
session required        pam_unix2.so
```

Comme étape finale, les modules de type session, rassemblés dans le fichier common-session, sont appelés pour configurer la session selon les paramètres de l'utilisateur en question. Même si pam_unix2 est à nouveau traité, en pratique, cela n'a pas de conséquence car son option none est indiquée dans pam_unix2.conf, le fichier de configuration correspondant à ce module. Le module pam_limits charge le fichier /etc/security/limits.conf, qui peut définir des limites d'utilisation de certaines ressources système. Les modules session sont appelés une deuxième fois lorsque l'utilisateur se délogue.

36.3 Configuration des modules PAM

Certains des modules PAM sont configurables. Les fichiers de configuration correspondants sont situés dans /etc/security. Cette section donne une brève description des fichiers de configuration appropriés pour l'exemple de sshd (pam_unix2.conf, pam_env.conf, pam_pwcheck.conf et limits.conf).

36.3.1 pam_unix2.conf

La méthode d'authentification classique utilisant les mots de passe est contrôlée par le module PAM pam_unix2. Il peut lire les données nécessaires dans /etc/passwd, /etc/shadow, les cartes NIS (Network Information Service - service d'informations réseau), les tables NIS+ ou une base de données LDAP. Le comportement de ce module peut être influencé soit par la configuration des options PAM de l'application elle-même, soit globalement via la modification du fichier /etc/security/pam_unix2.conf. Un fichier de configuration très simple pour le module est donné dans l'Exemple 36.6, « pam_unix2.conf » (p. 587).

***Exemple 36.6** pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        non
```

L'option `nullok` pour les modules de type `auth` et `password` indique que les mots de passe vides sont autorisés pour le type de compte correspondant. Les utilisateurs sont autorisés à changer les mots de passe de leur compte. L'option `none` pour le module de type `session` indique qu'aucun message n'est consigné au nom de ce module (paramétrage par défaut). Pour obtenir d'autres options de configuration, reportez-vous aux commentaires dans le fichier lui-même ainsi qu'à la page de manuel pam_unix2(8).

36.3.2 pam_env.conf

Ce fichier peut servir à définir un environnement standardisé pour les utilisateurs qui est paramétré chaque fois que le module `pam_env` est appelé. Grâce à lui, prédéfinissez les variables d'environnement à l'aide de la syntaxe suivante :

```
VARIABLE  [DEFAULT=[value]]  [OVERRIDE=[value]]
```

`VARIABLE`
Nom de la variable d'environnement à définir.

`[DEFAULT=[value]]`
Valeur par défaut que l'administrateur veut définir.

`[OVERRIDE=[value]]`
Valeurs qui peuvent faire l'objet d'une demande et qui sont définies par `pam_env`, ce qui écrase la valeur par défaut.

Un exemple type d'utilisation de `pam_env` est l'adaptation de la variable `DISPLAY`, qui est modifiée chaque fois qu'un login est exécuté à distance. Il est présenté dans l'Exemple 36.7, « pam_env.conf » (p. 587).

***Exemple 36.7** pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

La première ligne définit la valeur `localhost` pour la variable `REMOTEHOST`, qui est utilisée chaque fois que `pam_env` ne parvient pas à déterminer d'autre valeur. La

variable `DISPLAY` contient alors la valeur `REMOTEHOST`. Pour plus d'informations, reportez-vous aux commentaires dans le fichier `/etc/security/pam_env.conf`.

36.3.3 pam_pwcheck.conf

Ce fichier de configuration est destiné au module `pam_pwcheck`, qui lit les options dans ce fichier pour tous les modules de type `password`. Les paramètres enregistrés dans ce fichier sont prioritaires par rapport aux paramètres PAM d'une application individuelle. Si aucun paramètre propre à cette application n'a été défini, l'application utilise les paramètres globaux. L'Exemple 36.8, « pam_pwcheck.conf » (p. 588) indique à `pam_pwcheck` d'autoriser les mots de passe vides et les modifications de mots de passe. D'autres options pour ce module sont indiquées dans le fichier `/etc/security/pam_pwcheck.conf`.

***Exemple 36.8** pam_pwcheck.conf*

```
password:    nullok
```

36.3.4 limits.conf

Vous pouvez définir des limites système pour un utilisateur ou un groupe dans le fichier `limits.conf`, qui est lu par le module `pam_limits`. Ce fichier permet de définir soit des limites strictes (qu'il est absolument impossible d'outrepasser), soit des limites souples (qui peuvent être temporairement outrepassées). Pour plus d'informations sur la syntaxe et les options disponibles, reportez-vous aux commentaires inclus dans ce fichier.

36.4 Pour plus d'informations

Dans le répertoire `/usr/share/doc/packages/pam` de votre installation système, recherchez les documentations complémentaires suivantes :

LISEZMOI
: Au niveau supérieur de ce répertoire, il existe des fichiers LISEZMOI généraux. Le sous-répertoire `modules` contient les fichiers LISEZMOI relatifs aux modules PAM disponibles.

Linux-PAM System Administrators' Guide (Guide de l'administrateur système Linux-PAM)
: Ce document contient tout ce qu'un administrateur système doit connaître sur les modules PAM. Il traite de différents sujets, allant de la syntaxe des fichiers de configuration aux aspects de sécurité des modules PAM. Ce document est disponible au format PDF, HTML ou texte brut.

Linux-PAM Module Writers' Manual (Guide des rédacteurs de modules Linux-PAM)
: Ce document est un condensé de ce sujet destiné aux développeurs fournissant des informations sur la rédaction normalisée des modules PAM. Disponible au format PDF, HTML ou texte brut.

Linux-PAM Application Developers' Guide (Guide des développeurs d'application Linux-PAM)
: Ce document inclut tout ce qui est nécessaire à un développeur d'application qui veut utiliser les bibliothèques PAM. Disponible au format PDF, HTML ou texte brut.

Thorsten Kukuk a développé différents modules PAM pour SUSE Linux au sujet desquels il propose des informations sur le site `http://www.suse.de/~kukuk/pam/`.

37 Virtualisation avec Xen

Xen permet d'exécuter plusieurs systèmes LINUX sur une même machine physique. Le matériel associé aux différents systèmes est fourni sous forme virtuelle. Ce chapitre présente les possibilités et les limites de cette technologie, présentation complétée par les sections relatives à l'installation, la configuration et l'utilisation de Xen.

En général, les machines virtuelles doivent émuler le matériel nécessaire à l'exécution d'un système. L'inconvénient de cette technique tient au fait que le matériel émulé est bien plus lent que l'équipement d'origine. L'approche Xen est différente. L'émulation est limitée au plus petit nombre de composants possible. Pour y parvenir, Xen utilise la technique dite de *paravirtualisation*. Celle-ci consiste à présenter les machines virtuelles de manière similaire mais non identique au matériel sous-jacent. C'est ainsi, par exemple, que les systèmes d'exploitation hôtes et invités sont adaptés au niveau du kernel. L'espace utilisateur, quant à lui, reste inchangé. Xen contrôle le matériel à l'aide d'un hyperviseur et d'un invité de contrôle, également appelé domaine-0, qui fournissent l'ensemble des périphériques par blocs et réseau virtualisés requis. Les systèmes invités utilisent ces périphériques par blocs et réseau virtuels pour exécuter le système et se connecter à d'autres invités ou au réseau local. Lorsque plusieurs machines physiques exécutant Xen sont configurées de façon à ce que les périphériques par blocs et réseau virtuels soient disponibles, il est également possible de faire migrer un système invité d'un élément d'équipement vers un autre en cours d'exécution. À l'origine, Xen a été développé pour pouvoir exécuter jusqu'à 100 systèmes invités sur un même ordinateur, mais ce nombre est étroitement lié aux spécifications des systèmes hôtes actifs, et notamment à leur consommation de mémoire.

Afin de limiter la sollicitation de l'unité centrale, l'hyperviseur de Xen propose trois planificateurs distincts. Il est également possible de modifier le planificateur en cours d'exécution du système hôte, ce qui permet d'en modifier l'ordre de priorité. À

un niveau supérieur, la migration d'un invité peut aussi permettre d'ajuster la puissance de traitement disponible.

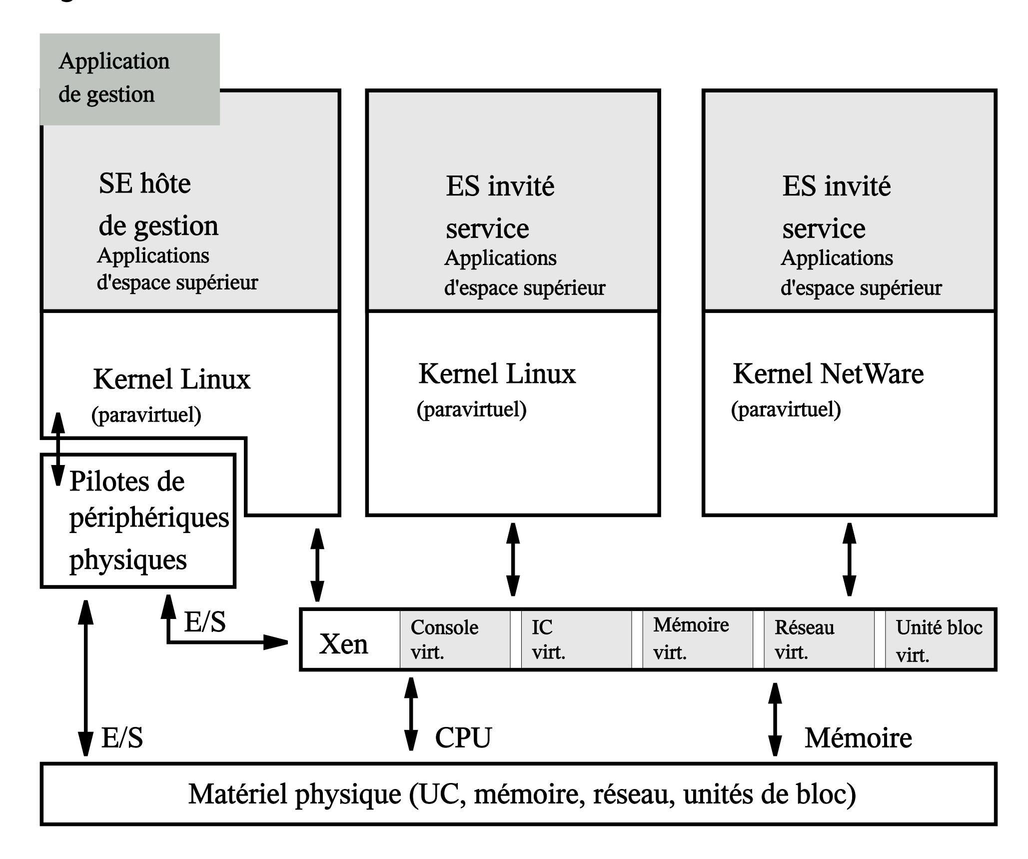
Le système de virtualisation Xen n'est pas sans certains inconvénients en ce qui concerne le matériel pris en charge :

- Plusieurs pilotes propriétaires, comme ceux commercialisés par Nvidia ou ATI, ne fonctionnent pas comme prévu. Dans ce cas, vous devez utiliser les pilotes libres disponibles, même s'ils ne prennent pas en charge toutes les capacités des composants. En outre, plusieurs puces WLAN et ponts CardBus ne sont pas pris en charge sous Xen.

- Dans la version 2, Xen ne prend pas en charge la technique PAE (Physical Adress Extension - extension d'adresses physiques) et est donc limité à 4 Go de mémoire.

- Le standard d'interface ACPI n'est pas pris en charge. La gestion d'énergie et les autres modes qui dépendent d'ACPI sont inopérants.

Figure 37.1 *Présentation de Xen*



37.1 Installation de Xen

La procédure d'installation de Xen passe par la configuration d'un domaine « domaine-0 » et l'installation des clients Xen. Vous devez d'abord vous assurer que les paquetages requis ont bien été installés. Il s'agit de `python`, `bridge-utils`, `xen` et d'un paquetage `kernel-xen`. Si vous utilisez des paquetages SUSE, Xen doit être ajouté à la configuration GRUB. Dans les autres cas, vous devez entrer des informations dans le fichier `boot/grub/menu.lst`. Cette entrée doit avoir l'aspect suivant :

```
title Xen2
    kernel (hd0,0)/boot/xen.gz dom0_mem=458752
    module (hd0,0)/boot/vmlinuz-xen <parameters>
    module (hd0,0)/boot/initrd-xen
```

Remplacez (hd0,0) par la partition qui contient votre répertoire `/boot`. Vous pouvez aussi consulter le Chapitre 29, *Chargeur d'amorçage* (p. 471). Modifiez la quantité de mémoire dom0_mem en fonction de votre système. La valeur maximum correspond à la capacité de votre mémoire système en Ko moins 65536. Remplacez <paramètres> par les paramètres utilisés normalement pour démarrer un kernel LINUX. Redémarrez ensuite le système en mode Xen. L'hyperviseur Xen est lancé au démarrage et le kernel LINUX est légèrement modifié, la plupart du matériel étant géré par le domaine-0. En dehors de ces exceptions, tout devrait fonctionner comme en mode normal.

37.2 Installation de domaines

L'installation et la configuration d'un domaine invité impliquent de suivre plusieurs procédures distinctes. Dans l'exemple qui suit, un premier domaine invité est installé et toutes les tâches nécessaires à la création d'une première connexion réseau sont effectuées.

Pour installer un système invité, vous devez fournir un système de fichiers racine dans un périphérique par blocs ou une image de système de fichiers, que vous devez ensuite configurer. Pour accéder ensuite à ce système, utilisez une console émulée ou configurez la connexion réseau pour cet invité. L'installation de SUSE Linux dans un répertoire est prise en charge par YaST. Les spécifications matérielles de ce type d'invité sont similaires à celles d'une installation normale de Linux.

Les domaines peuvent partager les systèmes de fichiers montés en lecture seule à partir de tous les domaines, comme `/usr` ou `/opt`. Ne partagez jamais un système de fichiers monté en lecture-écriture. Pour partager des données inscriptibles entre plusieurs domaines invités, utilisez NFS ou d'autres systèmes de fichiers montés en réseau ou en grappe.

AVERTISSEMENT: Démarrage d'un domaine invité

Lorsque vous démarrez un domaine invité, assurez-vous que les systèmes de fichiers de l'invité ne sont plus montés par un programme d'installation ni par le domaine-0 de contrôle.

La première chose à faire est de créer une image de système de fichiers dans laquelle est installé Linux pour l'invité :

1. Pour créer une image vide appelée `guest1` dans le répertoire `/var/tmp/` d'une taille de 4 Go, utilisez la commande suivante :

   ```
   dd if=/dev/zero of=/var/tmp/guest1 seek=1M bs=4096 count=1
   ```

2. L'image est simplement constituée d'un fichier volumineux et vide qui ne contient aucune information. Pour pouvoir y charger des fichiers, un système de fichiers est indispensable :

   ```
   mkreiserfs -f /var/tmp/guest1
   ```

   La commande `mkreiserfs` vous informe qu'il ne s'agit pas d'un périphérique par blocs spécial et vous demande de confirmer. Appuyez sur Y (pour Oui) puis sur Entrée pour continuer.

3. L'installation à proprement parler s'effectue dans un répertoire. L'image de système de fichiers `/var/tmp/guest1` doit donc être montée sur un répertoire :

   ```
   mkdir -p /var/tmp/dirinstall
   mount -o loop /var/tmp/guest1 /var/tmp/dirinstall
   ```

IMPORTANT

Une fois l'installation terminée, n'oubliez pas de redémonter l'image de système de fichiers. Lors de l'installation, YaST monte également le système de fichiers `/proc` que vous devez également démonter :

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall
```

37.2.1 Utilisation de YaST pour installer un domaine invité

Pour installer un domaine invité avec YaST, vous avez besoin de l'image de système de fichiers précédemment préparée pour le nouvel invité. Démarrez YaST et sélectionnez *Software (Logiciel) → Installation into Directory for XEN (Installation dans le répertoire pour XEN)*.

Le module YaST pour l'installation en répertoire propose diverses options qui doivent être paramétrées selon vos besoins :

- Target Directory (Répertoire cible) : `/var/tmp/dirinstall`

  Paramétrez cette option sur le point de montage de l'image de système de fichiers à utiliser. Le paramétrage par défaut est généralement acceptable.

- Run YaST and SuSEconfig at First Boot (Exécuter YaST et SuSEconfig au premier démarrage) : Yes (Oui)

  Paramétrez cette option sur *Yes* (Oui). Le système vous invite à indiquer un mot de passe racine et le nom du premier utilisateur lors du premier démarrage de l'invité.

- Create Image (Créer une image) : No (Non)

  L'image créée par cette option est simplement une archive tar du répertoire d'installation. Elle n'est pas utile ici.

- Software (Logiciel)

  Sélectionnez le type d'installation à utiliser. Le paramètre par défaut constitue normalement un bon choix de départ.

Cliquez sur *Next* (Suivant) pour démarrer l'installation. La procédure d'installation peut prendre un certain temps en fonction du nombre de paquetages utilisés. Une fois l'installation terminée, pensez à déplacer les bibliothèques tls :

```
mv /var/tmp/dirinstall/lib/tls /var/tmp/dirinstall/lib/tls.disabled
```

Xen utilise l'un des kernels installés dans le domaine-0 pour démarrer le domaine invité. Pour que vous puissiez utiliser la connexion en réseau dans le domaine invité, les modules de ce kernel doivent également être accessibles par l'invité.

```
cp -a /lib/modules/$(rpm -qf --qf %{VERSION}-%{RELEASE}-xen \
    /boot/vmlinuz-xen) /var/tmp/dirinstall/lib/modules
```

Pour éviter toute erreur système, l'image de système de fichiers doit être démontée à l'issue de l'installation :

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall/
```

Il serait possible de créer des kernels spécialisés pour le domaine-0, d'une part, et pour les systèmes invités, d'autre part. La différence principale tient au fait que les pilotes matériels ne sont pas nécessaires dans les systèmes invités. Comme ces pilotes sont

modulaires et qu'ils ne sont pas utilisés dans les systèmes invités, SUSE ne génère qu'un seul kernel pour les deux tâches.

37.2.2 Configuration d'un système de secours en tant que domaine invité

La manière la plus simple pour installer rapidement un système consiste à réutiliser un système de fichiers racine existant, comme le système de secours de SUSE Linux. Pour cela, il suffit d'échanger dans cette image l'image de kernel et les pilotes des périphériques par blocs et réseau virtuels. Pour simplifier encore cette procédure, vous pouvez utiliser le script `mk-xen-rescue-img.sh` disponible dans le répertoire `/usr/share/doc/packages/xen/`.

L'inconvénient inhérent à l'utilisation de la méthode de secours pour créer un système de fichiers racine tient au fait que le résultat ne contient pas de base de données RPM, ce qui complique l'ajout ultérieur de paquetages. Côté positif, le résultat est relativement peu volumineux et contient la plupart des éléments requis pour commencer la connexion en réseau.

Pour exécuter le script `mk-xen-rescue-img.sh`, vous avez au moins besoin du répertoire avec l'image de secours et d'un emplacement de destination pour l'image résultante. Par défaut, le répertoire se trouve sur le DVD d'amorçage, dans le répertoire `/boot`.

```
cd /usr/share/doc/packages/xen
./mk-xen-rescue-img.sh /media/dvd/boot /usr/local/xen 64
```

Le premier paramètre du script est le répertoire qui contient l'image de secours. Le deuxième paramètre est l'emplacement de destination du fichier image. Les paramètres facultatifs concernent les besoins en espace disque du domaine invité généré et la version de kernel à utiliser.

Le script copie ensuite l'image sur le nouvel emplacement, remplace le kernel et plusieurs modules de kernel, et désactive le répertoire `tls` dans le système. Pour terminer, il génère un fichier de configuration pour la nouvelle image dans `/etc/xen/`.

37.3 Configuration d'un domaine invité Xen

La documentation concernant la configuration d'un domaine invité n'est pas très exhaustive. La plupart des informations relatives à la configuration d'un domaine de ce type sont regroupées dans l'exemple de fichier de configuration /etc/xen/config. Les options requises sont expliquées, accompagnées d'une valeur par défaut ou au moins d'un exemple de configuration. Pour l'installation décrite dans Section 37.2.1, « Utilisation de YaST pour installer un domaine invité » (p. 595), créez un fichier /etc/xen/guest1 avec le contenu suivant :

```
kernel = "/boot/vmlinuz-xen"     ❶
ramdisk = "/boot/initrd-xen"     ❷
memory = 128                     ❸
name = "guest1"                  ❹
nics = "1"                       ❺
vif = [ 'mac=aa:cc:00:00:00:ab, bridge=xen-br0' ] ❻
disk = [ 'file:/var/tmp/guest1,hda1,w' ] ❼
root = "/dev/hda1 ro"            ❽
extra = "3"                      ❾
```

❶ Entrez le chemin d'accès au kernel Xen dans le domaine-0. Ce kernel sera exécuté ultérieurement dans le système invité.

❷ Sélectionnez le disque virtuel initial approprié qui contient les pilotes du kernel Xen. Sans cela, le kernel a tendance à « paniquer » car il est incapable de monter son système de fichiers racine.

❸ Indiquez la quantité de mémoire à affecter au domaine invité. Le système échoue s'il ne dispose pas de suffisamment de mémoire pour ses invités.

❹ Nom de l'invité.

❺ Nombre d'interfaces réseau virtuelles pour le domaine invité.

❻ Configuration de l'interface réseau virtuelle, y compris son adresse MAC et le pont auquel elle est connectée.

❼ Définissez ici les périphériques par blocs virtuels disponibles pour l'invité Xen. Pour utiliser des périphériques par blocs réels, créez des entrées comme ['phy:sdb1,hda1,w', 'phy:system/swap1,hda2,w'].

❽ Permet de définir le périphérique racine pour le kernel. Il doit s'agir du périphérique virtuel tel qu'il est vu par l'invité.

❾ Ajoutez ici des paramètres de kernel supplémentaires. Dans cet exemple, la valeur `3` signifie que l'invité est démarré au niveau d'exécution 3.

37.4 Démarrage et contrôle de domaines Xen

Pour pouvoir démarrer le domaine invité, l'hyperviseur Xen doit disposer de suffisamment de mémoire pour le nouvel invité. Commencez par vérifier la quantité de mémoire utilisée :

```
xm list
Name                  Id  Mem(MB)  CPU  State  Time(s)  Console
Domain-0               0      458    0  r----    181.8
```

S'il s'agit d'un ordinateur doté de 512 Mo de mémoire, l'hyperviseur Xen en utilise 64 Mo et le domaine-0 occupe le reste. Pour libérer une partie de la mémoire pour le nouvel invité, vous pouvez utiliser la commande `xm balloon`. Pour définir la taille du domaine-0 sur 330 Mo, entrez les indications suivantes sous `root` :

```
xm balloon 0 330
```

Dans la liste `xm list` qui apparaît ensuite, l'utilisation de la mémoire du domaine-0 devrait être tombée à 330 Mo. Vous disposez maintenant de suffisamment de mémoire pour démarrer un invité avec 128 Mo. La commande `xm start guest1 -c` démarre l'invité et associe la console de l'invité en phase de démarrage au terminal actuel. S'il s'agit du premier démarrage de l'invité en question, terminez l'installation avec YaST.

Il est toujours possible de détacher cette console ou de la rattacher à partir d'un autre terminal . Pour la détacher, utilisez la combinaison de touches Ctrl +]. Pour la rattacher, vérifiez d'abord l'ID de l'invité requis avec la commande `xm list` et associez la console à cet ID avec la commande `xm console` *ID*.

L'outil xm de Xen offre de nombreuses options de paramétrage. Vous pouvez afficher la liste des différents paramètres avec une brève explication en tapant `xm help`. Les commandes les plus importantes sont décrites dans le tableau (Tableau 37.1, « Commandes xm » (p. 600)) ci-dessous.

Tableau 37.1 Commandes xm

`xm help`	Permet d'imprimer la liste des commandes disponibles avec l'outil xm.
`xm console` *`ID`*	Permet de se connecter à la première console (tty1) de l'invité portant l'ID *`ID`*.
`xm balloon` *`ID Mem`*	Permet de paramétrer l'utilisation de la mémoire du domaine portant l'ID *`ID`* sur *`Mem`* en Mo.
`xm create` *`nomdom`* `[-c]`	Permet de démarrer le domaine avec le fichier de configuration *`nomdom`*. Le paramètre facultatif `-c` associe le terminal actuel à la première console tty du nouvel invité.
`xm shutdown` *`ID`*	Permet d'effectuer un arrêt normal de l'invité portant l'ID *`ID`*.
`xm destroy` *`ID`*	Permet de mettre fin immédiatement à l'exécution de l'invité portant l'ID *`ID`*.
`xm list`	Permet d'imprimer la liste de tous les domaines en cours d'exécution, avec leur ID, l'utilisation de la mémoire et leur temps UC respectifs.
`xm info`	Permet d'afficher des informations sur l'hôte Xen (UC et mémoire, par exemple).

37.5 Pour plus d'informations

Vous pourrez trouver des informations supplémentaires sur Xen sur les sites Web suivants :

- `file:/usr/share/doc/packages/xen/user/html/index.html` — Informations officielles pour les utilisateurs Xen. Nécessite le paquetage `xen-doc-html`.

- file:/usr/share/doc/packages/xen/interface/html/index.html — Documentation à caractère plus technique sur l'interface. Nécessite également le paquetage xen-doc-html.

- http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html — Page d'accueil de Xen proposant de nombreux liens vers d'autres documents.

- http://lists.xensource.com/ — Plusieurs listes de diffusion relatives à Xen.



Services

38 Bases de la mise en réseau

Linux offre les outils et fonctionnalités réseau nécessaires pour une intégration dans tout type de structure réseau. Le protocole Linux standard, TCP/IP, propose différents services et des fonctionnalités spéciales, présentés ici. Vous pouvez utiliser YaST pour configurer l'accès réseau via une carte réseau, un modem ou un autre périphérique. Vous pouvez également effectuer une configuration manuelle. Ce chapitre ne présente que les mécanismes fondamentaux et les fichiers de configuration associés.

Linux et les autres systèmes d'exploitation Unix utilisent tous le protocole TCP/IP. Il ne s'agit pas d'un protocole réseau unique mais d'un ensemble de protocoles réseau qui offre différents services. Les protocoles répertoriés dans le Tableau 38.1, « Différents protocoles de la famille TCP/IP » (p. 606) permettent l'échange de données entre deux ordinateurs via TCP/IP. Le terme « Internet » désigne l'ensemble des réseaux reliés par TCP/IP, qui constituent un véritable réseau mondial.

RFC signifie *Request for Comments* (demandes de commentaires). Les fichiers RFC sont des documents qui décrivent différents protocoles Internet et diverses procédures d'implémentation pour le système d'exploitation et ses applications. Les documents RFC décrivent la configuration des protocoles Internet. Pour en savoir plus sur un protocole, reportez-vous aux documents RFC correspondants. Ils sont accessibles en ligne, à l'adresse `http://www.ietf.org/rfc.html`.

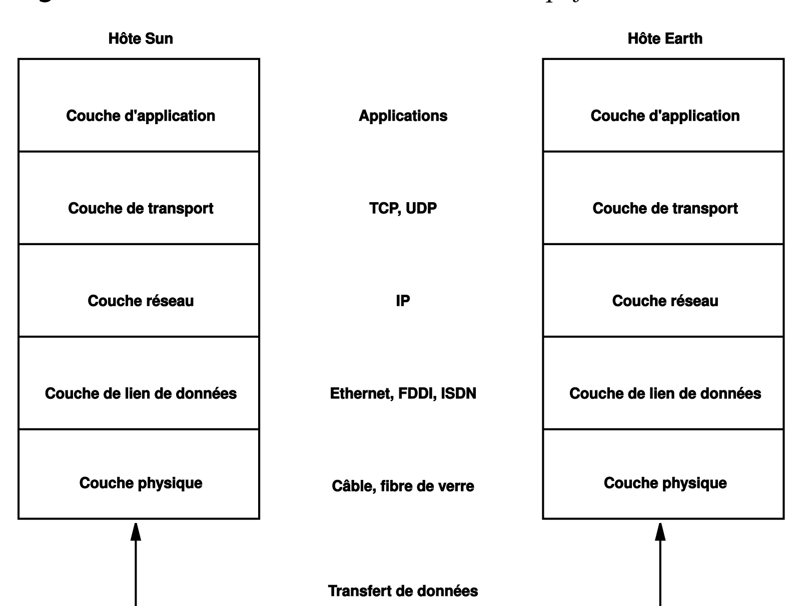
Tableau 38.1 *Différents protocoles de la famille TCP/IP*

Protocole	Description
TCP	Signifie « Transmission Control Protocol » (protocole de contrôle de transmission) : protocole sécurisé orienté connexion. Les données à transmettre sont d'abord envoyées par l'application sous forme de flux de données, puis converties au format approprié par le système d'exploitation. Les données parviennent à l'application voulue sur l'hôte cible, dans le format de flux de données dans lequel elles ont initialement été envoyées. TCP détermine si des données ont été perdues au cours de la transmission et sont arrivées dans le désordre. TCP est implémenté chaque fois que l'ordre des données est important.
UDP	Signifie « User Datagram Protocol » (protocole de diagramme utilisateur) : protocole non sécurisé sans connexion. Les données à transmettre sont envoyées sous forme de paquets générés par l'application. L'ordre dans lequel les données arrivent à destination n'est pas garanti et des pertes de données peuvent se produire. L'UDP convient aux applications orientées enregistrement. Il présente une période de latence plus courte que celle du protocole TCP.
ICMP	Signifie « Internet Control Message Protocol » (protocole de messages de contrôle Internet) : ce protocole n'est en général pas destiné à l'utilisateur final. Il s'agit d'un protocole de contrôle spécial qui génère des rapports d'erreurs et peut contrôler le comportement des ordinateurs impliqués dans le transfert de données TCP/IP. En outre, il offre un mode « echo » spécial qui peut être affiché à l'aide de la commande de programme Ping.
IGMP	Signifie « Internet Group Management Protocol » (protocole de gestion de groupe Internet) : ce protocole contrôle le comportement des ordinateurs lors de l'implémentation de la multidiffusion IP.

Comme l'illustre la Figure 38.1, « Modèle en couches TCP/IP simplifié » (p. 607), l'échange de données se déroule dans différentes couches. La couche réseau réelle correspond au transfert de données non sécurisé via IP (Internet protocol - protocole Internet). Par-dessus IP, TCP garantit, dans une certaine mesure, la sécurité du transfert des

données. La couche IP est prise en charge par le protocole sous-jacent dépendant du matériel (Ethernet, par exemple).

Figure 38.1 *Modèle en couches TCP/IP simplifié*

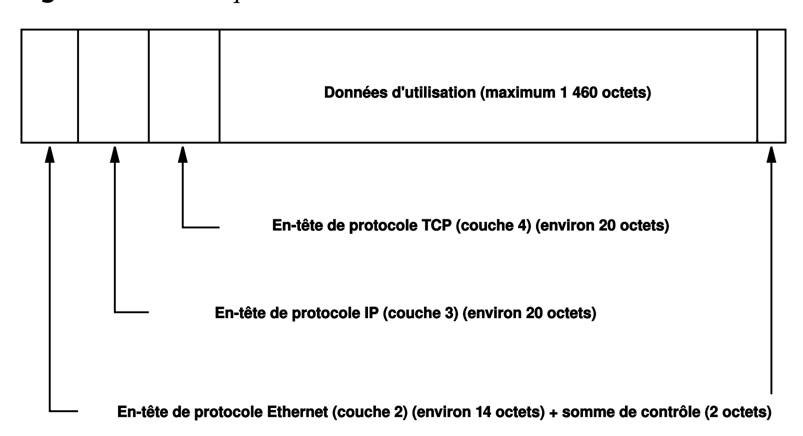


Le schéma ci-dessus fournit un ou deux exemples pour chaque couche. Les couches sont classées par *degré d'abstraction*. La couche inférieure est très proche des composants matériels. La couche supérieure, par contre, est presque entièrement abstraite et ne dépend pas du matériel. Chaque couche remplit une fonction bien précise. Les fonctions spéciales de chaque couche sont exprimées de manière relativement implicite dans leur description. La couche physique et celle de liaison de données représentent le réseau physique utilisé (Ethernet, par exemple).

Pratiquement tous les protocoles matériels reposent sur la notion de paquets. Les données à transmettre sont regroupées en *paquets*, car il est impossible de les envoyer en une seule fois. La taille maximum d'un paquet TCP/IP est d'environ 64 Ko. Les paquets sont généralement bien plus petits, en raison des limites imposées par le matériel réseau. La taille maximum d'un paquet de données sur un réseau Ethernet avoisine les 1,5 Ko. La taille d'un paquet TCP/IP est limitée à cette valeur lorsque les données sont envoyées sur un réseau Ethernet. Si la quantité de données transférées augmente, le système d'exploitation doit envoyer davantage de paquets de données.

Pour que les couches puissent exécuter les tâches qui leur reviennent, des informations supplémentaires concernant chaque couche doivent être enregistrées dans le paquet de données. Cette opération est réalisée dans l'*en-tête* du paquet. Chaque couche joint un petit bloc de données, appelé en-tête de protocole, à chaque paquet généré. La Figure 38.2, « Paquet TCP/IP sur Ethernet » (p. 608) illustre le déplacement d'un paquet de données TCP/IP sur un câble Ethernet. La somme de contrôle est située à la fin du paquet et non au début. Cela simplifie la tâche du matériel réseau.

Figure 38.2 *Paquet TCP/IP sur Ethernet*



Lorsqu'une application envoie des données sur le réseau, ces données passent par toutes les couches, qui sont toutes implémentées dans le kernel Linux, à l'exception de la couche physique. Chaque couche est chargée de préparer les données de manière à les transmettre à la couche suivante. La couche inférieure assure ensuite l'envoi des données. Pour la réception de données, la procédure est identique mais dans l'ordre inverse. Un peu comme les pelures d'un oignon, les en-têtes de protocoles sont supprimés, couche après couche, des données transmises. Enfin, la couche de transport se charge de mettre les données à disposition des applications cible. Ainsi, chaque couche communique uniquement avec la couche située directement au-dessus ou au-dessous d'elle. Pour les applications, le mode de transmission des données n'a aucune importance (via un réseau FDDI 100 Mbits/s ou une ligne modem 56 kbits/s, par exemple). De même, pour la ligne de données, peu importe le type des données transmises, tant que le format des paquets est correct.

38.1 Adresses IP et routage

Les informations de cette section concernent uniquement les réseaux IPv4. Pour obtenir des informations sur le protocole IPv6, successeur d'IPv4, consultez la Section 38.2, « IPv6 : Internet nouvelle génération » (p. 612).

38.1.1 Adresses IP

Chaque ordinateur connecté à Internet dispose d'une adresse 32 bits unique. Ces 32 bits (4 octets) sont généralement écrits comme l'illustre la deuxième ligne de l'Exemple 38.1, « Écriture d'adresses IP » (p. 609).

***Exemple 38.1** Écriture d'adresses IP*

```
Adress IP (format binaire):  11000000 10101000 00000000 00010100
Adress IP (format décimal):       192.     168.        0.      20
```

Sous forme décimale, les quatre octets sont écrits dans le système numérique décimal et sont séparés par un point. L'adresse IP est affectée à un hôte ou à une interface réseau. Elle ne peut être utilisée par aucun autre système dans le monde. Il y a des exceptions à cette règle, mais cela ne s'applique pas ici.

Les points figurant dans les adresses IP indiquent un système hiérarchique. Jusqu'aux années 1990, les adresses IP étaient réparties en classes bien distinctes. Toutefois, ce système, trop peu flexible, a été abandonné. Il est désormais remplacé par le *routage CIDR* (Classless InterDomain Routing - routage sans classes).

38.1.2 Masques réseau et routage

Les masques réseau permettent de définir la plage d'adresses d'un sous-réseau. Si deux hôtes figurent sur le même sous-réseau, ils peuvent se contacter directement ; s'ils se trouvent sur des sous-réseaux différents, ils ont besoin de l'adresse d'une passerelle, qui gère tout le trafic entre le sous-réseau et le reste du monde. Pour vérifier si deux adresses IP appartiennent au même sous-réseau, il vous suffit de les comparer au masque réseau à l'aide de l'opérateur « ET ». Si les résultats obtenus sont identiques, les deux adresses IP se trouvent sur le même réseau local. S'il existe des différences, l'adresse IP distante (et, par conséquent, l'interface distante) ne peut être atteinte que par le biais d'une passerelle.

Pour comprendre le fonctionnement du masque réseau, consultez l'Exemple 38.2, « Association d'adresses IP au masque réseau » (p. 610). Codé sur 32 bits, le masque réseau identifie le degré d'appartenance d'une adresse IP au réseau. Tous les bits à `1` indiquent que le bit correspondant dans l'adresse IP appartient au réseau. Les bits à `0` indiquent les bits membres du sous-réseau. Ainsi, plus le nombre de bits à `1` est important, plus le sous-réseau est restreint. Comme le masque réseau comporte toujours plusieurs bits à `1` successifs, il est également possible de compter simplement le nombre de bits de ce masque. Dans l'Exemple 38.2, « Association d'adresses IP au masque réseau » (p. 610), le premier réseau de 24 bits peut également être désigné comme suit : `192.168.0.0/24`.

Exemple 38.2 *Association d'adresses IP au masque réseau*

```
Adresse IP      (192.168.0.20) :  11000000 10101000 00000000 00010100
Masque réseau  (255.255.255.0) :  11111111 11111111 11111111 00000000
---------------------------------------------------------------------
Résultat de la liaison :          11000000 10101000 00000000 00000000
En notation décimale :                 192.     168.       0.       0

Adresse IP  (213.95.15.200) :     11010101 10111111 00001111 11001000
Masque réseau (255.255.255.0) :   11111111 11111111 11111111 00000000
---------------------------------------------------------------------
Résultat de la liaison :          11010101 10111111 00001111 00000000
En notation décimale :                 213.      95.      15.       0
```

Prenons un autre exemple : tous les ordinateurs connectés avec le même câble Ethernet se trouvent généralement sur le même sous-réseau et sont donc accessibles directement. Même si le sous-réseau est physiquement divisé par des commutateurs ou des ponts, il est toujours possible d'accéder directement à ces hôtes.

Les adresses IP situées hors du sous-réseau local ne sont accessibles que si une passerelle est configurée pour le réseau cible. Le plus souvent, une seule passerelle gère l'ensemble du trafic externe. Il est toutefois possible de configurer plusieurs passerelles pour les différents sous-réseaux.

Si une passerelle a été configurée, tous les paquets IP externes sont envoyés à la passerelle indiquée. Cette passerelle tente alors de transmettre les paquets de la même manière (d'hôte à hôte) jusqu'à ce qu'ils atteignent l'hôte cible ou que leur durée TTL (Time To Live - durée de vie) arrive à expiration.

Tableau 38.2 *Adresses particulières*

Type d'adresse	Description
Adresse réseau de base	Il s'agit du masque réseau associé (par ET) à une adresse quelconque du réseau (consultez l'Exemple 38.2, « Association d'adresses IP au masque réseau » (p. 610), sous `Résultat`). Cette adresse ne peut être assignée à aucun hôte.
Adresse de diffusion	Cette adresse correspond plus ou moins à l'instruction « accéder à tous les hôtes de ce sous-réseau ». Pour la générer, le masque réseau est inversé (au format binaire), puis associé à l'adresse réseau de base à l'aide de l'opérateur logique OU. L'exemple ci-dessus donne donc le résultat suivant : 192.168.0.255. Cette adresse ne peut être assignée à aucun hôte.
Hôte local	L'adresse `127.0.0.1` est affectée au « périphérique de bouclage (loopback) » de chaque hôte. Cette adresse permet de configurer une connexion avec votre propre ordinateur.

Les adresses IP devant être uniques au monde, vous ne pouvez pas simplement choisir des adresses aléatoires. Pour configurer un réseau IP privé, vous disposez de trois domaines d'adresses. Ces domaines ne pouvant pas être transmis sur Internet, ils ne permettent pas d'établir de connexion à partir des autres réseaux d'Internet. Ces domaines d'adresses (répertoriés dans le Tableau 38.3, « Domaines d'adresses IP privées » (p. 611)) sont définis dans le document RFC 1597.

Tableau 38.3 *Domaines d'adresses IP privées*

Réseau/Masque réseau	Domaine
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

38.2 IPv6 : Internet nouvelle génération

Avec l'émergence du Web (WWW - World Wide Web), Internet a connu une croissance explosive au cours des quinze dernières années, avec un nombre croissant d'ordinateurs qui communiquent via TCP/IP. Depuis l'invention du Web par Tim Berners-Lee (chercheur au CERN http://public.web.cern.ch) en 1990, le nombre d'hôtes Internet est passé de quelques milliers à près d'une centaine de millions.

Comme vous le savez déjà, une adresse IPv4 ne comprend que 32 bits. En outre, de nombreuses adresses IP sont perdues ; en effet, elles ne peuvent pas être utilisées en raison du mode d'organisation des réseaux. Le nombre d'adresses disponibles dans votre sous-réseau est égal à deux, puissance « nombre de bits », moins deux. Un sous-réseau dispose, par exemple, de 2, 6 ou 14 adresses. Ainsi, pour connecter 128 hôtes à Internet, vous avez besoin d'un sous-réseau comportant 256 adresses IP, parmi lesquelles seules 254 sont utilisables puisque deux sont réservées à la structure même du sous-réseau : l'adresse de diffusion et l'adresse réseau de base.

Avec le protocole IPv4 actuel, le DHCP ou le NAT (Network Address Translation - traduction des adresses réseau) sont les mécanismes standard utilisés pour pallier le manque potentiel d'adresses. Associées à la convention visant à séparer l'espace d'adressage public de l'espace d'adressage privé, ces méthodes permettent de réduire ce manque. Il existe toutefois un problème majeur : leur configuration est très complexe et exige énormément de maintenance. Pour configurer un hôte sur un réseau IPv4, vous avez besoin d'un certain nombre d'éléments d'adresse, tels que l'adresse IP de l'hôte, le masque de sous-réseau, l'adresse de passerelle et, parfois, une adresse de serveur de noms (DNS). Vous devez connaître tous ces éléments et vous ne pouvez pas les obtenir autrement.

Avec IPv6, finis les problèmes de pénurie d'adresses et de configuration complexe. Les sections suivantes traitent des améliorations et avantages offerts par IPv6, ainsi que du passage de l'ancien protocole au nouveau.

38.2.1 Avantages

L'avantage le plus flagrant et le plus important de ce nouveau protocole est l'augmentation considérable de l'espace d'adressage disponible. Une adresse IPv6 est composée

de valeurs 128 bits au lieu des 32 bits habituels. Cela représente plusieurs millions de milliards d'adresses IP possibles.

Cependant la taille n'est pas la seule différence entre les adresses IPv6 et IPv4. Les adresses IPv6 présentent également une structure interne différente, qui peut stocker des informations plus précises sur les systèmes et les réseaux auxquels elles appartiennent. Pour plus d'informations à ce sujet, consultez la Section 38.2.2, « Structures et types d'adresses » (p. 614).

Voici la liste des autres avantages du nouveau protocole :

Configuration automatique
IPv6 ajoute au réseau une fonction « Plug and Play » : tout système qui vient d'être configuré s'intègre au réseau (local) sans exiger de configuration manuelle. Le nouvel hôte utilise son mécanisme de configuration automatique pour dériver sa propre adresse à partir des informations mises à sa disposition par les routeurs voisins, en exploitant le protocole ND (*Neighbor Discovery* - repérage de voisinage réseau). Cette méthode n'exige aucune intervention de l'administrateur et rend inutile la gestion d'un serveur central pour l'allocation d'adresses ; il s'agit là d'un autre avantage par rapport à IPv4, pour lequel l'allocation d'adresses automatique requiert un serveur DHCP.

Mobilité
IPv6 rend possible l'assignation simultanée de plusieurs adresses à une même interface réseau. Les utilisateurs peuvent ainsi accéder facilement à plusieurs réseaux, ce qui s'apparente aux services d'accès mobile international offerts par les sociétés de téléphonie mobile : lorsque vous utilisez votre téléphone portable à l'étranger, il se connecte automatiquement au service de téléphonie du pays concerné, dès qu'il entre dans la zone correspondante ; où que vous soyez, vous pouvez être joint au même numéro et passer un appel comme si vous étiez chez vous.

Communication sécurisée
Avec IPv4 la sécurité réseau est toujours apportée par une fonction ajoutée. IPv6 compte, parmi ses fonctionnalités-clés, la fonction IPSec, qui permet à des systèmes de communiquer via un tunnel sécurisé afin d'éviter toute « écoute » par des intrus sur Internet.

Compatibilité avec les versions existantes
Il est évident qu'il serait irréaliste de vouloir faire passer l'ensemble d'Internet d'IPv4 vers IPv6 en une seule fois. Il est donc essentiel que ces deux protocoles puissent coexister, non seulement sur Internet mais aussi sur un même système. Cela est assuré

par l'utilisation d'adresses compatibles (les adresses IPv4 sont faciles à traduire en adresses IPv6) et l'emploi d'un certain nombre de tunnels. Voir Section 38.2.3, « Coexistence d'IPv4 et IPv6 » (p. 619). De plus, les systèmes peuvent exploiter la fonction de *double pile IP*, qui permet la prise en charge simultanée des deux protocoles, en leur attribuant deux piles réseau bien distinctes, de sorte qu'il n'y ait aucune interférence entre les deux versions.

La multidiffusion : des services sur mesure

Avec IPv4, certains services, comme SMB, doivent diffuser leurs paquets à tous les hôtes du réseau local. IPv6 offre une approche beaucoup plus élaborée : il permet aux serveurs de s'adresser aux hôtes par *multidiffusion*, c'est-à-dire de communiquer avec plusieurs hôtes en tant que groupe unique (par opposition à la communication avec tous les hôtes par *diffusion* ou avec chaque hôte par *diffusion individuelle*). Les hôtes qui peuvent être contactés en tant que groupe peut dépendre de l'application concernée. Il existe des groupes prédéfinis qui permettent de contacter tous les serveurs de noms (*groupe de multidiffusion vers tous les serveurs de noms*), par exemple, ou tous les routeurs (*groupe de multidiffusion vers tous les routeurs*).

38.2.2 Structures et types d'adresses

Comme indiqué précédemment, le protocole IP actuel a deux principaux points faibles : la pénurie d'adresses IP ne cesse de s'accentuer, et les tâches de configuration réseau et de gestion des tables de routage sont de plus en plus complexes et fastidieuses. IPv6 résout le premier problème en étendant l'espace d'adressage à 128 bits. Le deuxième inconvénient est résolu grâce à l'introduction d'une structure d'adresses hiérarchique, associée à des techniques élaborées d'allocation des adresses réseau, ainsi qu'à la fonction de *multihébergement* (possibilité d'assigner plusieurs adresses à un même périphérique, ce qui autorise l'accès à plusieurs réseaux).

Avec IPv6, il convient de connaître les trois différents types d'adresses suivants :

Diffusion individuelle

Les adresses de ce type sont associées à une seule et unique interface réseau. Les paquets comportant une telle adresse ne sont transmis qu'à une seule destination. Les adresses de diffusion individuelle sont, par conséquent, utilisées pour le transfert de paquets vers un hôte précis situé sur le réseau local ou sur Internet.

Multidiffusion

Les adresses de ce type sont associées à un groupe d'interfaces réseau. Les paquets comportant une telle adresse sont transmis à toutes les cibles membres du groupe. Les adresses de multidiffusion sont principalement utilisées par certains services réseau pour communiquer de manière correcte avec certains groupes d'hôtes.

Diffusion au membre le plus proche

Les adresses de ce type sont associées à un groupe d'interfaces. Les paquets comportant une telle adresse sont transmis au membre du groupe le plus proche de l'expéditeur, selon les critères du protocole de routage sous-jacent. Les adresses de diffusion au membre le plus proche permettent aux hôtes d'identifier plus facilement les serveurs qui offrent des services particuliers dans la zone réseau concernée. Tous les serveurs de même type portent la même adresse de diffusion au membre le plus proche. Lorsqu'un hôte émet une requête pour un service, il reçoit une réponse du serveur que le protocole de routage juge le plus proche. Si ce serveur rencontre un échec, le protocole sélectionne automatiquement le deuxième serveur le plus proche, puis le troisième, et ainsi de suite.

Une adresse IPv6 est composée de huit champs de quatre chiffres, représentant chacun 16 bits, notés sous forme hexadécimale. Ils sont également séparés par le caractère deux-points (`:`). Les zéros situés à gauche d'un champ donné peuvent être omis, mais pas les zéros qui apparaissent à l'intérieur ou à droite du champ. Une autre convention s'applique : un ou plusieurs groupes de quatre bits à zéro consécutifs peuvent être remplacés par un double caractère deux-points. Toutefois, le double deux-points (`::`) ne peut figurer qu'une seule fois dans chaque adresse. L'Exemple 38.3, « Exemple d'adresse IPv6 » (p. 615) illustre cette notation abrégée : les trois lignes qui y figurent représentent la même adresse.

***Exemple 38.3** Exemple d'adresse IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4 fe80 :
        : 10 : 1000 : 1a4
```

Chaque partie d'une adresse IPv6 a une fonction bien définie. Les premiers octets constituent le préfixe et indiquent le type d'adresse. La partie centrale correspond à la partie réseau de l'adresse (elle peut ne pas être utilisée). La fin de l'adresse identifie l'hôte. Avec IPv6, le masque réseau est défini en ajoutant à la fin de l'adresse une barre oblique, suivie de la longueur du préfixe. Dans l'Exemple 38.4, « Adresse IPv6 indiquant la longueur du préfixe » (p. 616), l'adresse contient les informations suivantes : les 64 premiers bits forment la partie réseau de l'adresse et les 64 derniers, la partie hôte.

Autrement dit, le nombre `64` signifie que le masque réseau comprend 64 bits à 1, en partant de la gauche. Comme avec IPv4, l'adresse IP est associée (par ET) aux valeurs du masque réseau afin de déterminer si l'hôte se trouve sur le même sous-réseau.

Exemple 38.4 *Adresse IPv6 indiquant la longueur du préfixe*

```
fe80::10:1000:1a4/64
```

IPv6 reconnaît plusieurs types de préfixes prédéfinis. Le Tableau 38.4, « Différents types de préfixes IPv6 » (p. 616) en reprend quelques-uns.

Tableau 38.4 *Différents types de préfixes IPv6*

Préfixe (hex)	Définition
`00`	Adresses IPv4 et adresses de compatibilité IPv4/IPv6. Servent à assurer la compatibilité avec IPv4. Leur utilisation nécessite toujours un routeur capable de traduire les paquets IPv6 en paquets IPv4. Plusieurs adresses spéciales, comme celle du périphérique de bouclage (loopback), comportent également ce préfixe.
`2` ou `3` comme premier chiffre	Adresses de diffusion individuelle globales pouvant être regroupées. Comme avec IPv4, une interface peut être assignée comme faisant partie d'un sous-réseau particulier. Actuellement, les espaces d'adressage suivants sont disponibles : `2001::/16` (espace d'adressage de qualité Production) et `2002::/16` (espace d'adressage IPv6 vers IPv4).
`fe80::/10`	Adresses « link-local » (à portée locale). Les adresses comportant ce préfixe ne doivent pas être routées et doivent, par conséquent, n'être accessibles qu'à partir du même sous-réseau.
`fec0::/10`	Adresses « site-local » (limitées au site). Ces adresses peuvent être routées, mais uniquement au sein du réseau de l'organisation à laquelle elles appartiennent. Elles sont en effet l'équivalent IPv6 de l'espace d'adressage réseau privé actuel (`10.x.x.x`, par exemple).
`ff`	Il s'agit d'adresses de multidiffusion.

Une adresse de diffusion individuelle est composée de trois éléments principaux :

Topologie publique
La première partie (qui contient également l'un des préfixes ci-dessus) sert au routage des paquets via le réseau Internet public. Elle comprend des informations sur la société ou l'institution qui fournit l'accès à Internet.

Topologie de site
La deuxième partie contient des informations de routage concernant le sous-réseau auquel transmettre le paquet.

ID d'interface
La troisième partie identifie l'interface à laquelle transmettre le paquet. Cela permet d'intégrer l'adresse MAC à l'adresse. Comme l'adresse MAC est un identificateur unique prédéfini codé dans le périphérique par le fabricant du matériel, la procédure de configuration est considérablement simplifiée. Les 64 premiers bits de l'adresse sont regroupés avec les 48 derniers bits de l'adresse MAC, ainsi qu'avec 24 bits restants qui contiennent des informations spéciales sur le type de jeton, afin de former le jeton `EUI-64`. Il est ainsi possible d'affecter un jeton `EUI-64` aux interfaces qui n'ont pas d'adresse MAC, comme les interfaces PPP ou RNIS.

Outre cette structure de base, IPv6 distingue cinq types d'adresses de diffusion individuelle :

`::` (non spécifié)
L'hôte utilise cette adresse comme adresse source lorsque l'interface est initialisée pour la première fois et qu'il est encore impossible de déterminer l'adresse d'une autre manière.

`::1` (boucle)
Adresse du périphérique de bouclage (loopback).

Adresses compatibles avec IPv4
L'adresse IPv6 est constituée de l'adresse IPv4 et d'un préfixe de 96 bits à zéro. Ce type d'adresse de compatibilité est utilisé pour le tunnelage (consultez la Section 38.2.3, « Coexistence d'IPv4 et IPv6 » (p. 619)), afin de permettre à des hôtes IPv4 et IPv6 de communiquer dans un environnement uniquement IPv4.

Adresses IPv4 assignées à IPv6
Ce type d'adresse indique une adresse IPv4 pure dans la notation IPv6.

Adresses locales

Deux types d'adresses sont possibles pour une utilisation locale :

« link-local » (à portée locale)

Ce type d'adresse ne peut être utilisé que dans le sous-réseau local. Les paquets comportant une adresse source ou cible de ce type ne doivent pas être routés vers Internet ou vers d'autres sous-réseaux. Ces adresses contiennent un préfixe spécial (`fe80::/10`) et l'ID d'interface de la carte réseau ; la partie centrale est composée de bits à zéro. Les adresses de ce type sont utilisées lors de la configuration automatique pour communiquer avec d'autres hôtes appartenant au même sous-réseau.

« site-local » (limitées au site)

Les paquets comportant ce type d'adresse peuvent être routés vers d'autres sous-réseaux, mais pas sur l'ensemble d'Internet : ils ne doivent pas sortir du réseau de l'organisation. Utilisées pour les réseaux Intranet, les adresses de ce type constituent un équivalent de l'espace d'adressage privé défini par IPv4. Elles contiennent un préfixe spécial (`fec0::/10`), l'ID d'interface et un champ de 16 bits indiquant l'ID du sous-réseau. Là encore, le reste de l'adresse est constitué de bits à zéro.

Une fonctionnalité entièrement nouvelle a fait son apparition avec IPv6 : chaque interface réseau comprend généralement plusieurs adresses IP, ce qui permet d'accéder à plusieurs réseaux via la même interface. Il est possible de configurer l'un de ces réseaux de manière entièrement automatique, à l'aide de l'adresse MAC et d'un préfixe connu : tous les hôtes du réseau local sont alors joignables dès qu'IPv6 est activé (en utilisant l'adresse « link-local »). Lorsqu'elle intègre l'adresse MAC, chaque adresse IP utilisée est unique au monde. Les seules parties variables de l'adresse sont celles indiquant la *topologie de site* et la *topologie publique*, qui dépendent du réseau réel sur lequel l'hôte fonctionne.

Pour aller et venir entre des réseaux différents, un hôte a besoin d'au moins deux adresses. L'une d'elles, l'*adresse d'origine*, contient non seulement l'ID d'interface mais aussi un identificateur du réseau privé auquel elle appartient normalement (avec le préfixe correspondant). L'adresse d'origine est une adresse statique et, en tant que telle, elle reste normalement inchangée. Malgré cela, tous les paquets destinés à l'hôte mobile peuvent lui être transmis, qu'il fonctionne sur le réseau privé ou en dehors. Cela est rendu possible par les nouvelles fonctionnalités qu'offre IPv6, telles que la *configuration automatique sans état* et le *ND (Neighbor Discovery - repérage du voisinage réseau)*. Outre son adresse d'origine, un hôte mobile comporte une ou plusieurs adresses sup-

plémentaires, qui appartiennent aux réseaux étrangers sur lesquels il se connecte par accès mobile. Ces adresses sont appelées adresses d'*hébergement temporaire* (care-of). Le réseau privé dispose d'une fonctionnalité qui transmet tous les paquets destinés à l'hôte lorsqu'il travaille en accès mobile. Dans un environnement IPv6, cette tâche est assurée par l'*agent privé*, qui récupère tous les paquets destinés à l'adresse d'origine et les retransmet via un tunnel. D'autre part, les paquets destinés à l'adresse d'hébergement temporaire (care-of) sont transférés directement à l'hôte mobile, sans autres détours.

38.2.3 Coexistence d'IPv4 et IPv6

La migration de tous les hôtes connectés à Internet d'IPv4 vers IPv6 est très progressive. Les deux protocoles vont coexister pendant encore assez longtemps. Sur un seul et même système, cette coexistence est garantie, à condition que les deux protocoles soient implémentés avec une *double pile*. Mais il reste certaines difficultés : comment un hôte IPv6 doit-il communiquer avec un hôte IPv4, et comment les paquets IPv6 peuvent-ils être acheminés par les réseaux actuels, en majorité de type IPv4. Les solutions les mieux adaptées sont notamment le tunnelage et les adresses de compatibilité (consultez la Section 38.2.2, « Structures et types d'adresses » (p. 614)).

Les hôtes IPv6, plus ou moins isolés sur le réseau IPv4 mondial peuvent communiquer via des tunnels : les paquets IPv6 sont encapsulés au format IPv4 pour pouvoir être transférés via un réseau IPv4. Une connexion de ce type entre deux hôtes IPv4 est appelée *tunnel*. Pour que cela soit possible, les paquets doivent comporter l'adresse cible IPv6 (ou le préfixe correspondant), ainsi que l'adresse IPv4 de l'hôte distant situé à l'extrémité réceptrice du tunnel. Vous pouvez configurer manuellement un tunnel simple, sur la base d'un accord passé entre les administrateurs des divers hôtes. Ce processus est appelé *tunnelage statique*.

Toutefois, la configuration et la maintenance des tunnels statiques exigent souvent trop de travail pour que cette solution puisse s'appliquer à des besoins de communication quotidiens. C'est pourquoi IPv6 fournit trois méthodes de *tunnelage dynamique* :

6over4 (IPv6 sur IPv4)

Les paquets IPv6 sont automatiquement encapsulés au format IPv4 et envoyés sur un réseau IPv4 possédant une fonction de multidiffusion. Le protocole IPv6 est alors amené à considérer l'ensemble du réseau (Internet) comme un immense réseau local (LAN). Cela rend possible la détermination automatique de l'extrémité réceptrice du tunnel IPv4. Toutefois, cette méthode est difficile à adapter, et la multidiffusion IP est loin d'être très répandue sur Internet. Il s'agit donc d'une solution

réservée aux petits réseaux d'entreprise et institutionnels qui utilisent la multidiffusion. Les spécifications de cette méthode sont exposées dans le document RFC 2529.

6to4 (IPv6 vers IPv4)
Avec cette méthode, les adresses IPv4 sont générées automatiquement à partir des adresses IPv6, ce qui permet aux hôtes IPv6 isolés de communiquer via un réseau IPv4. Cependant, de nombreux problèmes ont été signalés concernant la communication entre ces hôtes IPv6 isolés et Internet. Cette méthode est décrite dans le document RFC 3056.

IPv6 Tunnel Broker
Cette méthode repose sur des serveurs spéciaux, qui fournissent des tunnels dédiés pour les hôtes IPv6. Elle est décrite dans le document RFC 3053.

IMPORTANT: L'initiative 6bone

Il existe déjà, au coeur de l'« ancien » Internet, un réseau distribué global constitués de sous-réseaux IPv6 connectés par des tunnels. Il s'agit du réseau *6bone* (`http://www.6bone.net`), un environnement de test IPv6 que les programmateurs et les fournisseurs de services Internet peuvent utiliser pour développer et proposer des services IPv6, afin d'acquérir l'expérience nécessaire à l'implémentation du nouveau protocole. Pour plus d'informations, consultez le site Web du projet.

38.2.4 Configuration d'IPv6

Pour configurer IPv6, il devrait être inutile de modifier chaque poste de travail. Vous devez toutefois charger la fonction de prise en charge d'IPv6. Pour ce faire, entrez `modprobe ipv6` en vous connectant en tant qu'utilisateur `root`.

En raison du concept de configuration automatique d'IPv6, la carte réseau se voit assigner une adresse sur le réseau « *link-local* » (à portée locale). Normalement, aucune gestion des tables de routage n'a lieu sur un poste de travail. Le poste de travail peut envoyer des requêtes vers les routeurs réseau, à l'aide du *protocole d'annonce de routeur*, afin d'obtenir le préfixe et les passerelles à implémenter. Vous pouvez utiliser le programme radvd pour configurer un routeur IPv6. Ce programme indique aux stations de travail le préfixe à utiliser pour les adresses IPv6, ainsi que les routeurs nécessaires. Vous

pouvez également utiliser zebra pour la configuration automatique des adresses et du routage.

Pour obtenir des informations sur le mode de configuration de différents types de tunnels à l'aide des fichiers `/etc/sysconfig/network`, consultez la page de manuel ifup(8).

38.2.5 Pour plus d'informations

La présentation ci-dessus ne couvre pas tous les aspects du protocole IPv6. Pour approfondir vos connaissances, reportez-vous à la documentation en ligne et aux ouvrages suivants :

http://www.ngnet.it/e/cosa-ipv6.php
: Série d'articles fournissant une introduction claire aux concepts de base d'IPv6. Un bon moyen de commencer.

http://www.bieringer.de/linux/IPv6/
: Retrouvez ici la documentation HOWTO (Guide pratique) Linux concernant IPv6, ainsi que de nombreux liens sur le sujet.

http://www.6bone.net/
: Consultez ce site si vous souhaitez vous connecter à un réseau IPv6 avec tunnel.

http://www.ipv6.org/
: Point de départ de tout ce qui concerne IPv6.

RFC 2640
: Document RFC de référence pour IPv6.

IPv6 Essentials
: Cet ouvrage décrit tous les aspects importants d'IPv6 : *IPv6 Essentials*, par Silvia Hagen (ISBN 0-596-00125-8).

38.3 Résolution de noms

Le DNS (Domain Name System - système de noms de domaines) permet d'assigner une adresse IP à un ou plusieurs noms, et d'attribuer un nom à une adresse IP. Sous

Linux, cette conversion est généralement effectuée par un type de logiciel spécial, appelé BIND (Berkeley Internet Name Domain - domaine de noms Internet Berkeley). L'ordinateur en charge de cette conversion est appelé *serveur de noms*. Les noms constituent un système hiérarchique où les composants de nom sont séparés par un point. La hiérarchie de noms n'est toutefois pas dépendante de la hiérarchie d'adresses IP décrite ci-dessus.

Par exemple, imaginez un nom complet, comme `terre.exemple.com`, écrit au format `nomhôte.domaine`. Le nom complet (ou *nom de domaine complet* - FQDN) est composé d'un nom d'hôte et d'un nom de domaine (`exemple.com`). Ce dernier élément inclut également le *domaine de niveau supérieur* ou TLD (Top Level Domain), à savoir `com`.

L'assignation d'un domaine de niveau supérieur (TLD) est devenue très complexe, pour des raisons historiques. Les États-Unis utilisent traditionnellement des noms de domaine sur trois lettres. Par contre, le reste du monde utilise les codes de pays ISO sur deux lettres. En outre, des domaines de niveau supérieur plus longs ont été créés en 2000 afin de représenter certains types d'activités (par exemple, `.info`, `.name`, `.museum`).

Aux débuts d'Internet (avant 1990), le fichier `/etc/hosts` servait à stocker les noms de tous les ordinateurs présents sur Internet. Cela est très vite devenu peu pratique, compte tenu du nombre croissant d'ordinateurs connectés à Internet. C'est pourquoi une base de données décentralisée a été développée pour stocker les noms d'hôte de manière distribuée. Cette base de données, semblable au serveur de noms, ne tient pas les données concernant tous les hôtes d'Internet à disposition immédiate des utilisateurs, mais elle peut envoyer des requêtes à d'autres serveurs de noms.

Au sommet de la hiérarchie se trouvent les *serveurs de noms racine*. Ces serveurs de noms racine gèrent les domaines de niveau supérieur (TLD) et sont gérés par le NIC (Network Information Center - Centre d'informations sur les réseaux). Chaque serveur de noms racine connaît les serveurs de noms responsables d'un domaine de niveau supérieur (TLD) particulier. Pour plus d'informations sur les centres d'informations sur le réseau (NIC) des domaines de niveau supérieur, consultez le site `http://www.internic.net`.

Le DNS ne se contente pas de résoudre des noms d'hôte. Le serveur de noms identifie également l'hôte qui reçoit les messages électroniques pour l'intégralité d'un domaine (le serveur de messagerie (*mail exchanger (MX)*)).

Pour que votre ordinateur puisse résoudre une adresse IP, il doit connaître au moins un serveur de noms et son adresse IP. YaST vous permet de configurer facilement un serveur de noms. Si vous disposez d'une connexion à distance par modem, vous n'aurez peut-être même pas besoin de configurer manuellement un serveur de noms. Le protocole de connexion à distance fournit l'adresse du serveur de noms lors de l'établissement de la connexion. Pour savoir comment configurer l'accès au serveur de noms avec SUSE Linux, consultez le Chapitre 40, *La résolution de noms* (p. 655).

Le protocole `WHOIS` est étroitement associé au DNS. Ce programme vous permet de trouver rapidement le serveur responsable d'un domaine donné.

38.4 Configuration d'une connexion réseau avec YaST

Linux prend en charge de nombreux types de connexions réseau. La plupart d'entre elles utilisent des noms de périphérique différents et les fichiers de configuration sont répartis dans plusieurs emplacements du système de fichiers. Pour obtenir un aperçu détaillé des aspects de la configuration réseau manuelle, consultez la Section 38.5, « Configuration manuelle d'une connexion réseau » (p. 635).

Lors de l'installation, vous pouvez utiliser YaST pour configurer automatiquement toutes les interfaces qui ont été détectées. Après l'installation, vous pouvez à tout moment configurer d'autres équipements sur le système installé. Les sections suivantes décrivent la configuration réseau de tous les types de connexions réseau pris en charge par SUSE Linux.

38.4.1 Configuration de la carte réseau avec YaST

Après le démarrage du module, YaST affiche une boîte de dialogue générale sur la configuration réseau. La partie supérieure affiche la liste de toutes les cartes réseau à configurer. Toute carte correctement détectée est listée avec son nom. Pour configurer les périphériques qui n'ont pas été détectés, cliquez sur *Autre (non détecté)*, comme indiqué dans la section intitulée « Configuration manuelle d'une carte réseau non détectée » (p. 624). La partie inférieure comporte la liste des périphériques déjà configurés, avec

le type de réseau et l'adresse. Vous pouvez maintenant configurer une nouvelle carte réseau ou modifier une configuration existante.

Configuration manuelle d'une carte réseau non détectée

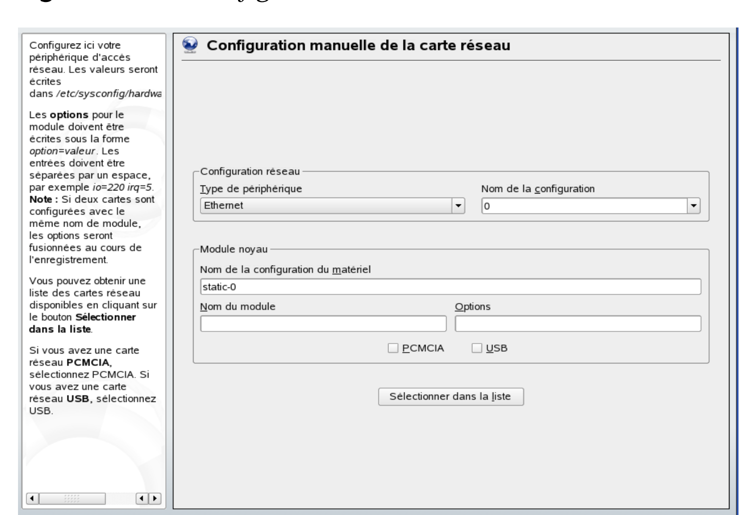
La configuration d'une carte réseau qui n'a pas été détectée (listée comme *Autre*) inclut les éléments suivants :

Configuration réseau
Définissez le type de périphérique de l'interface parmi les options proposées, ainsi que le nom de la configuration. Vous trouverez des informations sur les conventions de dénomination des fichiers de configuration dans la page du manuel sur `getcfg(8)`.

Module de kernel
L'option *Nom de la configuration du matériel* indique le nom du fichier `/etc/sysconfig/hardware/hwcfg-*` qui contient les paramètres matériels de votre carte réseau. Ce fichier contient le nom du module de kernel approprié ainsi que les options nécessaires pour initialiser le matériel. YaST propose généralement des noms judicieux pour les périphériques PCMCIA et USB. Pour tout autre matériel, `hwcfg-static-0` n'est utile que si la carte est configurée avec le nom `0`.

Si la carte réseau est un périphérique PCMCIA ou USB, cochez les cases correspondantes, puis cliquez sur *Suivant* pour quitter cette boîte de dialogue. Sinon, sélectionnez votre modèle de carte réseau dans *Sélectionner dans la liste*. YaST choisit alors automatiquement le module de kernel adapté à la carte. Fermez la boîte de dialogue en cliquant sur *Suivant*.

Figure 38.3 Configuration de la carte réseau



Configuration de l'adresse réseau

Définissez le type de périphérique de l'interface et le nom de la configuration. Sélectionnez le type de périphérique parmi les options proposées. Spécifiez un nom de configuration selon vos besoins. Les paramètres par défaut sont généralement utiles et peuvent être acceptés. Vous trouverez des informations sur les conventions de dénomination des fichiers de configuration dans la page du manuel sur `getcfg(8)`.

Si vous avez sélectionné *sans fil* comme type de périphérique de l'interface, configurez le mode de fonctionnement, le nom du réseau (ESSID) et le codage dans la boîte de dialogue suivante, *Configuration de la carte réseau sans fil*. Cliquez sur *OK* pour achever la configuration de la carte. Vous trouverez une description détaillée de la configuration des cartes WLAN dans la Section 22.1.3, « Configuration avec YaST » (p. 316). Pour tous les autres types d'interfaces, poursuivez avec la configuration de l'adresse réseau :

Configuration automatique d'adresses (via DHCP)

Si votre réseau comporte un serveur DHCP, vous pouvez l'utiliser pour configurer automatiquement votre adresse réseau. Vous pouvez également utiliser cette option si votre fournisseur d'accès ADSL n'attribue pas d'adresse IP statique à votre système. Si vous décidez d'utiliser le protocole DHCP, configurez les détails après avoir

sélectionné *Options du client DHCP*. Déterminez si le serveur DHCP doit toujours répondre aux demandes de diffusion et indiquez l'identificateur à utiliser. Par défaut, les serveurs DHCP utilisent l'adresse matérielle de la carte pour identifier une interface. Si vous disposez d'une configuration d'hôte virtuel où plusieurs hôtes communiquent via la même interface, vous devez les distinguer à l'aide d'identificateurs.

Configuration de l'adresse statique
Activez cette option si vous disposez d'une adresse statique. Saisissez ensuite l'adresse et le masque de sous-réseau correspondant à votre réseau. Le masque de sous-réseau prédéfini répond généralement aux exigences d'un réseau privé standard.

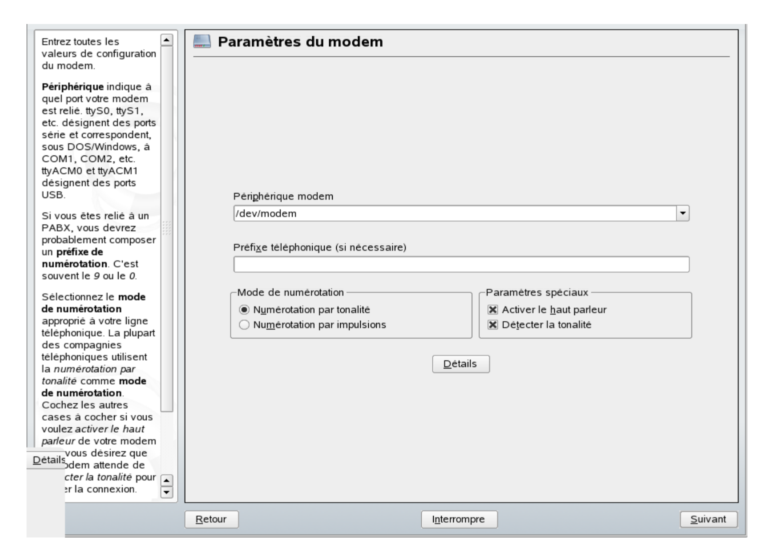
Pour quitter cette boîte de dialogue, cliquez sur *Suivant*. Vous pouvez également continuer et configurer le nom d'hôte, le serveur de noms et les détails de routage (consultez les sections Serveur DNS (↑Démarrage) et Routage (↑Démarrage)).

L'option *Avancé* permet de spécifier des paramètres plus complexes. Dans *Paramètres détaillés*, utilisez *Contrôlé par l'utilisateur* pour déléguer le contrôle de la carte réseau depuis l'administrateur (`root`) à l'utilisateur normal. Dans le contexte d'une utilisation mobile, ceci permet à l'utilisateur d'adapter plus facilement les différentes connexions réseau, puisqu'il peut contrôler l'activation ou la désactivation de l'interface. Cette boîte de dialogue permet également de définir la MTU (Maximum Transmission Unit - unité de transmission maximum) et le type d'*activation du périphérique*.

38.4.2 Modem

Dans le centre de contrôle YaST, le menu *Périphériques réseau* permet d'accéder à la configuration du modem. Si votre modem n'a pas été détecté automatiquement, ouvrez la boîte de dialogue de configuration manuelle. Dans la boîte de dialogue qui apparaît, saisissez l'interface à laquelle est connecté le modem dans *Modem*.

Figure 38.4 Configuration du modem



Si votre ligne passe par un PABX, vous devrez sans doute indiquer un préfixe. C'est généralement un zéro. Pour le savoir, consultez les instructions relatives à votre PABX. De plus, choisissez entre la numérotation par tonalité et par impulsions. Vous pouvez également décider si la sortie son du modem doit être activée et si vous souhaitez attendre la tonalité. N'activez pas cette dernière option si le modem est connecté à un autocommutateur.

Dans *Détails*, définissez le débit en bauds et les chaînes d'initialisation du modem. Vous ne devez modifier ces paramètres que si votre modem n'a pas été détecté automatiquement ou si des paramètres particuliers sont nécessaires à la transmission des données. C'est notamment le cas pour les adaptateurs terminaux RNIS. Pour quitter cette boîte de dialogue, cliquez sur *OK*. Pour déléguer le contrôle du modem à l'utilisateur normal sans autorisation root, activez l'option *Contrôlé par l'utilisateur*. De cette manière, un utilisateur sans autorisation administrateur peut activer ou désactiver une interface. Dans le champ *Expression régulière du préfixe de numérotation*, indiquez une expression régulière. Dans KInternet, l'option *Préfixe de numérotation*, que l'utilisateur normal peut modifier, doit correspondre à cette expression régulière. Si vous laissez ce champ vide, l'utilisateur ne peut pas définir un autre *préfixe de numérotation* sans autorisation administrateur.

Dans la boîte de dialogue suivante, sélectionnez le fournisseur d'accès Internet (ISP - Internet service provider). Sélectionnez *Pays* pour afficher la liste des ISP en activité

dans votre pays. Vous pouvez également cliquer sur *Nouveau* pour ouvrir une boîte de dialogue dans laquelle vous saisissez les informations sur votre ISP. Il s'agit notamment du nom de la connexion à distance et de l'ISP, mais aussi du login et du mot de passe fournis par l'ISP. Activez l'option *Toujours demander le mot de passe* pour que votre mot de passe soit demandé à chaque connexion.

Dans la dernière boîte de dialogue, vous pouvez paramétrer des options de connexion supplémentaires :

Connexion à la demande
Définissez au moins un serveur de noms si vous activez cette option.

Modifier DNS une fois connecté
Cette option est activée par défaut, ce qui a pour effet de mettre à jour l'adresse du serveur de noms chaque fois que vous vous connectez à Internet.

Retrouver automatiquement le DNS
Si le fournisseur ne transmet pas son serveur de noms de domaine après la connexion, désactivez cette option et saisissez manuellement les données concernant le serveur de noms.

Mode stupide
Cette option est activée par défaut. Grâce à elle, les invites de saisie envoyées par le serveur de l'ISP sont ignorées, ce qui les empêche d'interférer avec le processus de connexion.

Interface pare-feu externe* et *Redémarrer le pare-feu
Ces options vous permettent d'activer SUSEfirewall2, qui vous protège contre les attaques extérieures pendant toute la durée de votre connexion Internet.

Délai d'inactivité (secondes)
Cette option permet d'indiquer le délai d'inactivité réseau au bout duquel le modem se déconnecte automatiquement.

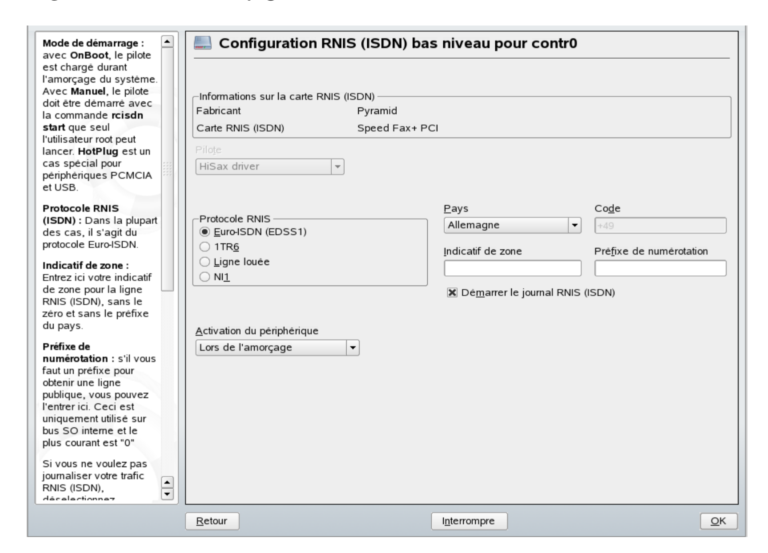
Détails IP
Cette option ouvre la boîte de dialogue de configuration de l'adresse. Si votre ISP n'attribue pas d'adresse IP dynamique à votre hôte, désactivez l'option *Adresse IP dynamique*, puis entrez l'adresse IP locale de l'hôte et l'adresse IP distante. Demandez ces informations à votre ISP. Laissez l'option *Route par défaut* activée, puis cliquez sur *OK* pour fermer la boîte de dialogue.

Cliquez sur *Suivant* pour revenir à la première boîte de dialogue, qui affiche un résumé de la configuration du modem. Cliquez sur *Terminer* pour fermer la boîte de dialogue.

38.4.3 RNIS

Utilisez ce module pour configurer une ou plusieurs cartes RNIS dans votre système. Si YaST n'a pas détecté votre carte RNIS, sélectionnez-la manuellement. Vous pouvez utiliser plusieurs interfaces et plusieurs ISP peuvent être configurés pour une seule interface. Les boîtes de dialogue suivantes permettent de définir les options RNIS nécessaires au fonctionnement correct de la carte.

Figure 38.5 *Configuration RNIS*



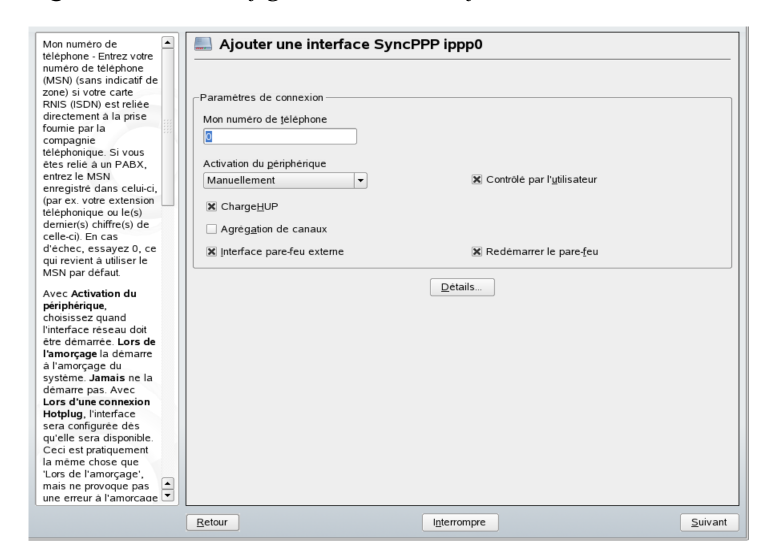
Dans la boîte de dialogue suivante, représentée dans la Figure 38.5, « Configuration RNIS » (p. 629), sélectionnez le protocole à utiliser. Le protocole par défaut est *Euro-ISDN (EDSS1)*, mais pour les systèmes téléphoniques antérieurs ou pour les installations de grande envergure, sélectionnez *1TR6*. Si vous êtes aux États-Unis, sélectionnez *NI1*. Sélectionnez votre pays dans le champ prévu à cet effet. Le code du pays approprié apparaît alors dans le champ de saisie. Pour finir, saisissez votre *indicatif de zone* et le *préfixe de numérotation* si nécessaire.

L'option *Mode de démarrage* permet de définir le mode de démarrage de l'interface RNIS : Si vous sélectionnez *Lors de l'amorçage*, le pilote RNIS est initialisé à chaque

démarrage du système. Si vous sélectionnez *Manuellement*, vous devez charger le pilote RNIS en tant qu'utilisateur `root` à l'aide de la commande `rcisdn start`. Si vous sélectionnez l'option *Lors d'une connexion Hotplug*, utilisée pour les périphériques PCMCIA ou USB, le pilote se charge après le branchement du périphérique. Une fois ces paramètres définis, sélectionnez *OK*.

La boîte de dialogue suivante permet d'indiquer le type d'interface de votre carte RNIS et d'ajouter des ISP à une interface existante. Les interfaces peuvent être de type `SyncPPP` ou `RawIP`, mais la plupart des ISP utilisent le mode `SyncPPP` décrit ci-dessous.

Figure 38.6 *Configuration de l'interface RNIS*



Le numéro à saisir dans le champ *Mon numéro de téléphone* dépend de votre installation :

La carte RNIS est branchée directement à la prise téléphonique
: Une ligne RNIS standard fournit trois numéros de téléphone, appelés MSN (Multiple Subscriber Numbers - numéros multiples). Si l'abonné en demande davantage, il peut en obtenir jusqu'à 10. Vous devez saisir ici l'un de ces numéros, sans indicatif régional. Si vous ne saisissez pas le bon numéro, votre opérateur revient automatiquement au premier MSN attribué à votre ligne RNIS.

La carte RNIS est reliée à un PABX
: Ici aussi, la configuration peut dépendre de l'équipement installé :

1. Les petits autocommutateurs privés (PABX) conçus pour un usage privé utilisent généralement le protocole Euro-ISDN (EDSS1) pour les appels internes. Ces installations sont équipées d'un bus S0 interne et utilisent des numéros internes pour les appareils connectés.

   Utilisez l'un des numéros internes en tant que numéro MSN. Vous devez être en mesure d'utiliser au moins un des MSN du PABX qui ont été activés pour l'accès direct au réseau téléphonique. Si cela ne fonctionne pas, essayez le 0. Pour plus d'informations, consultez la documentation fournie avec votre PABX.

2. Les grands autocommutateurs conçus pour les entreprises utilisent en principe le protocole 1TR6 pour les appels internes. Leur MSN est appelé EAZ et correspond généralement au numéro d'accès direct. Pour une configuration sous Linux, il suffit normalement de saisir le dernier chiffre de l'EAZ. En dernier recours, essayez tous les chiffres de 1 à 9.

Activez l'option *ChargeHUP* pour que la connexion se termine juste avant l'unité suivante de facturation. Toutefois, cette possibilité n'est pas offerte par tous les ISP. Vous pouvez également activer l'agrégation de canaux (Multilink PPP) en sélectionnant l'option correspondante. Enfin, vous pouvez sélectionner *Interface pare-feu externe* et *Redémarrer le pare-feu* pour activer SUSEfirewall2 sur votre connexion. Sélectionnez l'option *Contrôlé par l'utilisateur* pour permettre à l'utilisateur normal sans autorisation administrateur d'activer ou de désactiver l'interface.

Cliquez sur *Détails* pour ouvrir une boîte de dialogue dans laquelle vous pouvez implémenter des schémas de connexion qui ne concernent pas les particuliers. Pour quitter la boîte de dialogue *Détails*, sélectionnez *OK*.

La boîte de dialogue suivante vous permet de paramétrer l'adresse IP. Si votre ISP ne vous a pas fourni d'adresse IP statique, sélectionnez *Adresse IP dynamique*. Dans le cas contraire, saisissez l'adresse IP locale de votre hôte ainsi que l'adresse IP distante dans les champs correspondants, selon les caractéristiques de votre ISP. Si vous souhaitez utiliser cette interface comme route par défaut vers Internet, sélectionnez *Route par défaut*. Un hôte ne peut avoir qu'une interface configurée comme route par défaut. Pour quitter cette boîte de dialogue, sélectionnez *Suivant*.

La boîte de dialogue suivante vous permet d'indiquer votre pays et de sélectionner votre fournisseur d'accès. Les ISP de la liste sont tous de type « sans abonnement ». Si votre ISP ne figure pas dans la liste, sélectionnez *Nouveau*. La boîte de dialogue *Paramètres du fournisseur* qui apparaît permet de saisir tous les renseignements sur votre ISP.

Lorsque vous saisissez le numéro de téléphone, n'incluez aucun espace ni aucune virgule entre les chiffres. Enfin, saisissez le login et le mot de passe fournis par votre ISP. Une fois que vous avez terminé, cliquez sur *Suivant*.

Pour utiliser l'option *Connexion à la demande* sur un poste de travail autonome, indiquez également le serveur de noms (serveur DNS). La plupart des fournisseurs d'accès gèrent le DNS dynamique, ce qui signifie que l'adresse IP d'un serveur de noms est transmise par l'ISP chaque fois que vous vous connectez. Toutefois, pour un poste de travail isolé, vous devez encore fournir une adresse fictive, telle que `192.168.22.99`. Si votre ISP ne prend pas en charge le DNS dynamique, indiquez les adresses IP du serveur de noms de votre ISP. Si vous le souhaitez, fixez le timeout de la connexion, c'est-à-dire la période d'inactivité réseau (en secondes) au terme de laquelle la connexion doit être automatiquement désactivée. Pour confirmer les paramètres choisis, cliquez sur *Suivant*. YaST affiche un résumé des interfaces configurées. Cliquez sur *Terminer* pour activer tous ces paramètres.

38.4.4 Modem câble

Dans certains pays (Autriche, États-Unis), l'accès à Internet par le réseau de télévision par câble est très répandu. L'abonné au réseau câblé reçoit généralement un modem relié d'une part au câble TV et d'autre part à la carte réseau d'un ordinateur, à l'aide d'un câble 10Base-T (paire torsadée). Le modem câble fournit alors une connexion Internet dédiée, associée à une adresse IP fixe.

Lors de la configuration de la carte réseau, suivez les instructions de votre ISP et sélectionnez *Configuration automatique d'adresses (via DHCP)* ou *Configuration de l'adresse statique*. Aujourd'hui, la plupart des fournisseurs d'accès utilisent le protocole DHCP. En général, l'adresse IP statique fait partie d'une offre spéciale pour entreprise.

38.4.5 DSL

Pour configurer votre périphérique DSL, sélectionnez le module *DSL* dans la section *Périphériques réseau* de YaST. Ce module YaST est composé de plusieurs boîtes de dialogue qui permettent de définir les paramètres des connexions DSL en fonction de l'un des protocoles suivants :

- PPPoE (PPP via Ethernet)

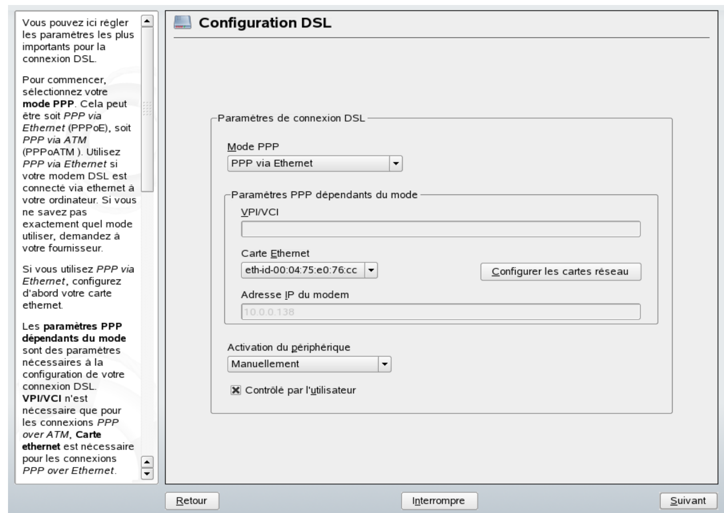
- PPPoATM (PPP via ATM)
- CAPI pour ADSL (cartes Fritz)
- PPTP (Point-to-Point Tunneling Protocol) - Autriche

La configuration d'une connexion DSL basée sur le protocole PPPoE ou PPTP exige la configuration correcte de la carte réseau correspondante. Si ce n'est pas le cas, sélectionnez *Configurer les cartes réseau* pour configurer votre carte réseau (consultez la Section 38.4.1, « Configuration de la carte réseau avec YaST » (p. 623)). Dans le cas d'une liaison DSL, les adresses peuvent être attribuées automatiquement mais pas via DHCP. C'est pourquoi vous ne devez pas activer l'option *Configuration automatique d'adresses (via DHCP)*. En revanche, saisissez une adresse statique fictive pour l'interface, telle que `192.168.22.1`. Dans *Masque de sous-réseau*, saisissez `255.255.255.0`. Si vous configurez un poste de travail autonome, laissez le champ *Passerelle par défaut* vide.

ASTUCE

Les valeurs des champs *Adresse IP* et *Masque de sous-réseau* ne sont que des marques de réservation. Elles servent uniquement à initialiser la carte réseau et ne représentent pas la liaison DSL en tant que telle.

Figure 38.7 *Configuration DSL*



Pour démarrer la configuration DSL (consultez la Figure 38.7, « Configuration DSL » (p. 633)), choisissez d'abord le mode PPP et la carte Ethernet à laquelle le modem DSL est connecté (il s'agit en général de `eth0`). Utilisez ensuite l'option *Activation du périphérique* pour indiquer si la liaison DSL doit être établie lors du processus d'amorçage. Cliquez sur *Contrôlé par l'utilisateur* pour permettre à l'utilisateur standard sans autorisation administrateur d'activer ou de désactiver l'interface avec KInternet. Cette boîte de dialogue vous permet également de sélectionner votre pays et de faire votre choix parmi les ISP présents. Les détails des boîtes de dialogue suivantes dépendent des options définies jusqu'ici. C'est pourquoi ils ne sont que brièvement mentionnés dans les paragraphes suivants. Pour en savoir plus sur les options disponibles, lisez l'aide détaillée fournie dans les boîtes de dialogue.

Pour utiliser l'option *Connexion à la demande* sur un poste de travail autonome, indiquez également le serveur de noms (serveur DNS). La plupart des fournisseurs d'accès gèrent le DNS dynamique. Ainsi, l'adresse IP d'un serveur de noms est transmise par l'ISP chaque fois que vous vous connectez. Toutefois, pour un poste de travail isolé, fournissez une adresse fictive, telle que `192.168.22.99`. Si votre ISP ne prend pas en charge le DNS dynamique, saisissez l'adresse IP du serveur de noms fournie par votre ISP.

L'option *Délai d'inactivité (secondes)* définit la période d'inactivité du réseau au terme de laquelle la connexion doit être automatiquement désactivée. Choisissez de préférence une valeur comprise entre 60 et 300 secondes. Si l'option *Connexion à la demande* est désactivée, il est préférable de définir le timeout sur zéro afin d'éviter le raccrochage automatique.

La configuration d'une connexion T-DSL est très similaire à celle de DSL. Il vous suffit de sélectionner *T-Online* comme fournisseur d'accès et YaST ouvre la boîte de dialogue qui permet de configurer la connexion T-DSL. Dans cette boîte de dialogue, vous pouvez fournir les informations supplémentaires nécessaires à la connexion T-DSL, telles que l'identificateur de ligne, le numéro T-Online, le code d'utilisateur et votre mot de passe. Toutes ces informations figurent dans la documentation que vous avez reçue après vous être abonné à T-DSL.

38.5 Configuration manuelle d'une connexion réseau

La configuration manuelle des logiciels réseau doit toujours être la dernière alternative. Il est recommandé d'utiliser YaST. Toutefois, ces informations générales sur la configuration réseau peuvent également vous aider à utiliser YaST.

Toutes les cartes réseau intégrées et les cartes réseau à chaud (PCMCIA, USB, certaines cartes PCI) sont détectées et configurées via la fonctionnalité d'enfichage à chaud. Le système considère la carte réseau de deux manières : tout d'abord comme un périphérique physique et en second lieu, comme une interface. L'insertion ou la détection d'un périphérique déclenche un événement d'enfichage à chaud. Cet événement déclenche l'initialisation du périphérique avec le script `hwup`. Lorsque la carte réseau est initialisée en tant que nouvelle interface réseau, le kernel génère un autre événement d'enfichage à chaud qui déclenche la configuration de l'interface avec `ifup`.

Le kernel numérote les noms d'interface en fonction de leur date d'enregistrement. L'ordre d'initialisation est déterminant pour l'attribution des noms. Si l'une des cartes réseau est défaillante, la numérotation de toutes les cartes initialisées par la suite est modifiée. Pour les cartes réellement enfichables à chaud, il faut tenir compte de l'ordre de connexion des périphériques.

Pour obtenir une configuration flexible, la configuration des périphériques (matériel) et des interfaces a été séparée, et l'association des configurations à leurs périphériques et interfaces ne dépend plus du nom des interfaces. La configuration des périphériques est située dans `/etc/sysconfig/hardware/hwcfg-*`. La configuration des interfaces se trouve dans `/etc/sysconfig/network/ifcfg-*`. Le nom des fichiers de configuration est attribué de façon à décrire leurs périphériques et interfaces respectifs. L'association précédente entre pilotes et noms d'interface nécessitait des noms d'interface statiques. Cette association ne peut donc plus avoir lieu dans `/etc/modprobe.conf`. Avec le nouveau concept, des déclarations d'alias dans ce fichier provoqueraient des effets secondaires indésirables.

Les noms des configurations (tout ce qui suit `hwcfg-` ou `ifcfg-`) peuvent décrire les périphériques à l'aide du connecteur, d'un identifiant propre au périphérique ou du nom de l'interface. Par exemple, le nom de configuration d'une carte PCI pourrait être `bus-pci-0000:02:01.0` (connecteur PCI) ou `vpid-0x8086-0x1014-0x0549`

(ID fabricant et ID produit). Le nom de l'interface associée pourrait être bus-pci-0000:02:01.0 ou wlan-id-00:05:4e:42:31:7a (adresse MAC).

Pour assigner une configuration réseau à une carte d'un type donné (dont une seule peut être insérée à la fois) plutôt qu'à une carte donnée, sélectionnez des noms de configuration moins spécifiques. Par exemple, bus-pcmcia peut être utilisé pour toutes les cartes PCMCIA. D'autre part, les noms peuvent être limités par l'utilisation du type d'interface. Par exemple, wlan-bus-usb pourrait désigner les cartes WLAN connectées à un port USB.

Le système utilise toujours la configuration qui décrit le mieux une interface ou le périphérique qui fournit l'interface. La commande getcfg permet de rechercher la meilleure configuration possible. Le résultat de getcfg fournit toutes les informations utiles pour décrire un périphérique. Les détails sur les noms de configuration sont disponibles à la page du manuel qui porte sur getcfg.

La méthode décrite permet de configurer correctement une interface réseau même si les périphériques réseau ne sont pas toujours initialisés dans le même ordre. Toutefois, le nom de l'interface dépend toujours de l'ordre d'initialisation. Il existe deux manière de garantir un accès fiable à l'interface d'une carte réseau donnée :

- getcfg-interface *nom de la configuration* retourne le nom de l'interface réseau associée. Par conséquent, le nom de configuration, tel que pare-feu, dhcpd, routage ou différentes interfaces réseau virtuelles (tunnels), peut être saisi dans certains fichiers de configuration à la place du nom d'interface, qui n'est pas persistant.

- Vous pouvez assigner des noms d'interface persistants à toutes les interfaces dont les fichiers de configuration n'incluent pas de nom d'interface. Pour cela, utilisez les déclarations PERSISTENT_NAME=*pname* dans un fichier de configuration d'interface (ifcfg-*). Toutefois, le nom persistant *pname* ne doit pas être identique au nom automatiquement attribué par le kernel. Par conséquent, eth*, tr*, wlan*, etc., ne sont pas autorisés. Utilisez plutôt net* ou des noms descriptifs comme externe, interne ou dmz. Vous ne pouvez assigner un nom persistant à une interface qu'immédiatement après son enregistrement, ce qui impose de recharger le pilote de la carte réseau ou d'exécuter hwup *description du périphérique* . La commande rcnetwork restart ne suffit pas pour remplir cette fonction.

IMPORTANT: Utilisation de noms d'interface persistants

L'utilisation de noms d'interface persistants n'a pas été testée dans tous les domaines. Par conséquent, certaines applications risquent de ne pas être en mesure de gérer les noms d'interface librement choisis.

La commande `ifup` exige une interface existante puisqu'elle n'initialise pas le matériel. La commande `hwup` (exécutée par `hotplug` ou `coldplug`) gère l'initialisation du matériel. Lorsqu'un périphérique est initialisé, `hotplug` exécute automatiquement la commande `ifup` pour la nouvelle interface qui est configurée si le mode de démarrage est `onboot`, `hotplug` ou `auto` et si le service `network` a été démarré. Auparavant, la commande `ifup` *`nom d'interface`* déclenchait l'initialisation du matériel. Désormais, la procédure est inversée. Un composant matériel est d'abord initialisé, puis toutes les autres actions suivent. Vous pouvez ainsi configurer un nombre variable de périphériques de manière optimale avec un ensemble de configurations existant.

Le Tableau 38.5, « Scripts de configuration réseau manuelle » (p. 637) récapitule les principaux scripts impliqués dans la configuration réseau. Dans la mesure du possible, la distinction a été faite entre matériel et interface.

Tableau 38.5 *Scripts de configuration réseau manuelle*

Étape de configuration	Commande	Fonction
Matériel	`hw{up,down,status}`	Les scripts `hw*` sont exécutés par le sous-système d'enfichage à chaud pour initialiser un périphérique, annuler son initialisation ou demander l'état d'un périphérique. Pour plus d'informations, reportez-vous à la page du manuel qui porte sur `hwup`.
Interface	`getcfg`	Vous pouvez utiliser la commande `getcfg` pour demander le nom d'interface associé au nom d'une configuration ou à la description d'un matériel. Pour plus d'informations,

Étape de configuration	Commande	Fonction
		reportez-vous à la page du manuel qui porte sur `getcfg`.
Interface	`if{up,down,status}`	Les scripts `if*` démarrent les interfaces réseau existantes ou retournent l'état de l'interface spécifiée. Pour plus d'informations, reportez-vous à la page du manuel qui porte sur `ifup`.

Pour plus d'informations sur les noms de périphérique enfichables à chaud et persistants, consultez le Chapitre 32, *Le système Hotplug* (p. 535) et le Chapitre 33, *Noeuds de périphériques dynamiques avec* `udev` (p. 543).

38.5.1 Fichiers de configuration

Cette section présente les fichiers de configuration réseau, et explique leur fonction et le format utilisé.

/etc/syconfig/hardware/hwcfg-*

Ces fichiers contiennent les configurations matérielles des cartes réseau et d'autres périphériques. Ils contiennent les paramètres nécessaires, tels que le module de kernel, le mode de démarrage et les associations de scripts. Pour plus d'informations, reportez-vous à la page du manuel qui porte sur `hwup`. Quel que soit le matériel existant, les configurations `hwcfg-static-*` sont appliquées lors du démarrage de coldplug.

/etc/sysconfig/network/ifcfg-*

Ces fichiers contiennent les configurations de l'interface réseau. Ils incluent notamment des informations telles que le mode de démarrage et l'adresse IP. Les paramètres possibles sont décrits dans la page du manuel qui porte sur `ifup`. En outre, vous pouvez utiliser toutes les variables des fichiers `dhcp`, `wireless` et `config` dans les fichiers `ifcfg-*` si un paramétrage général doit être utilisé pour une seule interface.

/etc/sysconfig/network/config, dhcp, wireless

Le fichier `config` contient les paramètres généraux relatifs au comportement des commandes `ifup`, `ifdown` et `ifstatus`. Le fichier `dhcp` contient les paramètres relatifs à DHCP et le fichier `wireless`, les paramètres concernant les cartes LAN sans fil. Les variables des trois fichiers de configuration sont commentées et vous pouvez également les utiliser dans les fichiers `ifcfg-*`, où elles sont prioritaires.

/etc/sysconfig/network/routes,ifroute-*

Le routage statique des paquets TCP/IP est déterminé ici. Vous pouvez saisir toutes les routes statiques requises par les différentes tâches système dans le fichier `/etc/sysconfig/network/routes` : routes vers un hôte, routes vers un hôte via une passerelle et routes vers un réseau. Définissez un fichier de configuration supplémentaire pour chaque interface nécessitant un routage individuel : `/etc/sysconfig/network/ifroute-*`. Remplacez `*` par le nom de l'interface. Les déclarations des fichiers de configuration du routage ont l'aspect suivant :

```
# Destination     Fictif/Passerelle     Masque réseau            Périphérique
#
127.0.0.0          0.0.0.0            255.255.255.0      lo
204.127.235.0      0.0.0.0            255.255.255.0      eth0
default            204.127.235.41     0.0.0.0            eth0
207.68.156.51      207.68.145.45      255.255.255.255    eth1
192.168.0.0        207.68.156.51      255.255.0.0        eth1
```

La destination de la route apparaît dans la première colonne. Celle-ci peut contenir l'adresse IP d'un réseau ou d'un hôte ou, en cas de serveurs de noms *accessibles*, le réseau ou le nom d'hôte complet.

La deuxième colonne contient la passerelle par défaut ou une passerelle permettant d'accéder à un hôte ou à un réseau. La troisième colonne contient le masque réseau pour les réseaux ou les hôtes placés derrière une passerelle. Par exemple, le masque est `255.255.255.255` pour un hôte placé derrière une passerelle.

La quatrième colonne n'est utile que pour les réseaux connectés à l'hôte local, tels que la boucle, Ethernet, RNIS, PPP et le périphérique factice. Vous devez saisir le nom du périphérique ici.

Vous pouvez utiliser une cinquième colonne (facultative) pour spécifier le type d'une route. Les colonnes inutiles doivent contenir le signe moins (–) pour garantir que l'analyseur interprète correctement la commande. Pour plus d'informations, reportez-vous à la page du manuel qui porte sur routes(5).

/etc/resolv.conf

Ce fichier indique le domaine auquel appartient l'hôte (mot-clé search). L'état de l'adresse du serveur de noms auquel vous devez accéder y figure également (mot-clé nameserver). Vous pouvez spécifier plusieurs noms de domaine. En cas de résolution d'un nom qui n'est pas complet, le système tente d'en générer un en reliant les différents éléments search. Pour utiliser plusieurs serveurs de noms, saisissez plusieurs lignes, chacune débutant par nameserver. Faites précéder les commentaires du caractère #. YaST entre le serveur de noms spécifié dans ce fichier. L'Exemple 38.5, « /etc/resolv.conf » (p. 640) illustre à quoi /etc/resolv.conf peut ressembler.

Exemple 38.5 *Exemple 38.5 /etc/resolv.conf*

```
# Notre domaine
search exemple.com
#
# Nous utilisons sun (192.168.0.20) comme serveur de noms
nameserver 192.168.0.20
```

Certains services, tels que pppd (wvdial), ipppd (isdn), dhcp (dhcpcd et dhclient), pcmcia et hotplug, modifient le fichier /etc/resolv.conf à l'aide du script modify_resolvconf. Si le fichier /etc/resolv.conf a été temporairement modifié par ce script, il contient un commentaire prédéfini qui fournit des informations sur le service qui l'a modifié, l'endroit où le fichier d'origine a été sauvegardé et le moyen de désactiver le mécanisme de modification automatique. Si /etc/resolv.conf est modifié plusieurs fois, le fichier inclut les modifications successives. Vous pouvez revenir sur ces modifications si l'annulation a lieu dans un ordre différent de celui dans lequel les modifications ont été introduites. Parmi les services susceptibles d'avoir besoin de cette flexibilité figurent isdn, pcmcia et hotplug.

Si un service n'a pas été arrêté comme il se doit, vous pouvez utiliser le fichier modify_resolvconf pour restaurer le fichier d'origine. En outre, à l'amorçage du système, un contrôle permet de vérifier s'il existe un fichier resolv.conf modifié ou non

nettoyé, par exemple à la suite d'un crash système, auquel cas le fichier resolv.conf d'origine (non modifié) est restauré.

YaST utilise la commande modify_resolvconf check pour savoir si le fichier resolv.conf a été modifié. Il avertit ensuite l'utilisateur que ses modifications seront perdues après la restauration du fichier. À l'exclusion de cet aspect, YaST n'a pas recours au fichier modify_resolvconf. Par conséquent, la modification de resolv.conf via YaST a le même impact que n'importe quelle modification manuelle. Dans les deux cas, l'effet des modifications est permanent. Les modifications demandées par les services mentionnés ne sont que temporaires.

/etc/hosts

Dans ce fichier, illustré dans l'Exemple 38.6, « /etc/hosts » (p. 641), les adresses IP sont assignées aux noms d'hôte. Si aucun serveur de noms n'est implémenté, tous les hôtes vers lesquels une connexion IP doit être configurée doivent être listés ici. Pour chaque hôte, saisissez une ligne composée de l'adresse IP, du nom d'hôte complet et du nom d'hôte dans le fichier. L'adresse IP doit être placée en début de ligne et les éléments doivent être séparés par des espaces et des tabulations. Les commentaires sont toujours précédés du caractère #.

Exemple 38.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.0.20 sun.exemple.com sun
192.168.0.0 earth.exemple.com earth
```

/etc/networks

Ici, les noms de réseau sont convertis en adresses réseau. Leur format est similaire à celui du fichier hosts, si ce n'est que les noms de réseau précèdent les adresses. (voir Exemple 38.7, « /etc/networks » (p. 641)).

Exemple 38.7 */etc/networks*

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

Ce fichier contrôle la résolution de noms (conversion des noms d'hôte et de réseau via la bibliothèque du *résolveur*). Il est exclusivement utilisé pour les programmes liés aux bibliothèques libc4 ou libc5. Pour les programmes glibc actuels, reportez-vous aux paramètres de `/etc/nsswitch.conf`. Un paramètre doit toujours être seul dans sa propre ligne. Les commentaires sont précédés du caractère `#`. Le Tableau 38.6, « Paramètres de /etc/host.conf » (p. 642) indique les paramètres disponibles. Un exemple de fichier `/etc/host.conf` est présenté dans l'Exemple 38.8, « /etc/host.conf » (p. 643).

Tableau 38.6 *Paramètres de /etc/host.conf*

order *hosts*, *bind*	Indique l'ordre d'accès aux services pour la résolution du nom. Les arguments disponibles sont les suivants (séparés par des espaces ou des virgules) : *hosts* : lance la recherche dans le fichier `/etc/hosts` *bind* : accède à un serveur de noms *nis* : utilise NIS
multi *on*/*off*	Détermine si un hôte saisi dans `/etc/hosts` peut avoir plusieurs adresses IP.
nospoof *on* spoofalert *on*/*off*	Ces paramètres ont un impact sur la prévention de la *simulation* du serveur de noms, mais n'ont pas d'autre effet sur la configuration réseau.
trim *nom de domaine*	Le nom de domaine spécifié est séparé du nom d'hôte après la résolution de ce dernier (tant que le nom d'hôte inclut le nom de domaine). Cette option est utile si le fichier `/etc/hosts` contient uniquement des noms issus du domaine local, mais qui doivent malgré tout être reconnus avec les noms de domaine associés.

Exemple 38.8 */etc/host.conf*

```
# named est en cours d'exécution
order hosts bind
# Autoriser plusieurs adresses
multi on
```

/etc/nsswitch.conf

La bibliothèque C version 2.0 de GNU a introduit le *NSS* (Name Service Switch – Commutation de service de noms). Pour plus d'informations, reportez-vous à la page du manuel qui porte sur `nsswitch.conf(5)` et au manuel *The GNU C Library Reference Manual*.

L'ordre des requêtes est déterminé dans le fichier `/etc/nsswitch.conf`. Un exemple de fichier `nsswitch.conf` est présenté dans l'Exemple 38.9, « /etc/nsswitch.conf » (p. 643). Les commentaires sont précédés du caractère `#`. Dans cet exemple, l'élément situé sous la base de données `hosts` signifie qu'une requête est envoyée à `/etc/hosts` (`files`) via DNS (consultez le Chapitre 40, *La résolution de noms* (p. 655)).

Exemple 38.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Les « bases de données » disponibles sur NSS sont listées dans le Tableau 38.7, « Bases de données disponibles via /etc/nsswitch.conf » (p. 644). De plus, `automount`, `bootparams`, `netmasks` et `publickey` sont prévus dans un futur proche. Les options de configuration des bases de données NSS sont listées dans le Tableau 38.8, « Possibilités de configuration des « bases de données » NSS » (p. 644).

Tableau 38.7 Bases de données disponibles via /etc/nsswitch.conf

`aliases`	Alias de messagerie implémentés par `sendmail` ; consultez la page du manuel `man 5 aliases`.
`ethers`	Adresses Ethernet.
`group`	Pour les groupes d'utilisateurs ; utilisée par `getgrent`. Consultez également la page du manuel qui porte sur `group`.
`hosts`	Pour les noms d'hôte et les adresses IP ; utilisée par `gethostbyname` et les fonctions similaires.
`netgroup`	Listes des utilisateurs et hôtes valides sur le réseau, dans le but de contrôler les autorisations d'accès. Consultez la page du manuel qui porte sur `netgroup(5)`.
`networks`	Adresses et noms des réseaux ; utilisée par `getnetent`.
`passwd`	Mots de passe utilisateur ; utilisée par `getpwent` ; consultez la page du manuel qui porte sur `passwd(5)`.
`protocols`	Protocoles réseau ; utilisée par `getprotoent` ; consultez la page du manuel qui porte sur `protocols(5)`.
`rpc`	Noms et adresses d'appels de procédure distants ; utilisée par `getrpcbyname` et les fonctions similaires.
`services`	Services réseau ; utilisée par `getservent`.
`shadow`	Mots de passe shadow des utilisateurs ; utilisée par `getspnam` ; consultez la page du manuel qui porte sur `shadow(5)`.

Tableau 38.8 Possibilités de configuration des « bases de données » NSS

`files`	accès direct aux fichiers (par exemple, `/etc/aliases`)
`db`	accès via une base de données

`nis`, `nisplus`	NIS ; consultez également le Chapitre 41, *Utilisation de NIS* (p. 677)
`dns`	uniquement utilisée en tant qu'extension de `hosts` et `networks`
`compat`	uniquement utilisée en tant qu'extension de `passwd`, `shadow` et `group`

/etc/nscd.conf

Ce fichier permet de configurer nscd (name service cache daemon - démon cache de service de noms). Consultez les pages du manuel qui portent sur `nscd(8)` et `nscd.conf(5)`. Par défaut, les entrées système de `passwd` et `groups` sont mises en cache par nscd. Ceci est important pour les performances des services Annuaire, tels que NIS et LDAP puisque, sinon, la connexion réseau doit être utilisée pour chaque accès aux noms ou aux groupes. `hosts` n'est pas mis en cache par défaut puisque le mécanisme de nscd qui permet de mettre les hôtes en cache rend le système local incapable de se fier aux recherches directes et inverses. Configurez un serveur de cache DNS au lieu de demander à nscd de mettre les noms en mémoire cache.

Si la mise en cache de `passwd` est activée, la reconnaissance d'un nouvel utilisateur local prend environ 15 secondes. Pour réduire ce temps d'attente, redémarrez nscd à l'aide de la commande `rcnscd restart`.

/etc/HOSTNAME

Il contient le nom d'hôte sans le nom de domaine associé. Ce fichier est lu par plusieurs scripts lors du démarrage de la machine. Il peut contenir uniquement une ligne dans laquelle le nom d'hôte est défini.

38.5.2 Scripts de démarrage

En plus des fichiers de configuration décrits précédemment, il existe différents scripts qui chargent les programmes réseau lors du démarrage de la machine. Ces programmes démarrent dès que le système passe à l'un des *niveaux d'exécution multi-utilisateurs*.

Certains de ces scripts sont décrits dans le tableau Tableau 38.9, « Quelques scripts de démarrage des programmes réseau » (p. 646).

Tableau 38.9 *Quelques scripts de démarrage des programmes réseau*

`/etc/init.d/network`	Ce script gère la configuration des interfaces réseau. Le matériel doit déjà avoir été initialisé par `/etc/init.d/coldplug` (via `hotplug`). Si le service `network` n'a pas été démarré, aucune interface réseau n'est implémentée lors de son ajout via hotplug.
`/etc/init.d/inetd`	Démarre le service xinetd, qui permet de rendre les services de serveur disponibles sur le système. Par exemple, il peut démarrer vsftpd dès l'établissement d'une connexion FTP.
`/etc/init.d/portmap`	Démarre portmapper dont le serveur RPC a besoin (un serveur NFS, par exemple).
`/etc/init.d/nfsserver`	Démarre le serveur NFS.
`/etc/init.d/sendmail`	Contrôle le processus sendmail.
`/etc/init.d/ypserv`	Démarre le serveur NIS.
`/etc/init.d/ypbind`	Démarre le client NIS.

38.6 smpppd comme assistant de connexion

La plupart des particuliers n'ont pas de ligne dédiée à la connexion Internet. Ils utilisent donc une connexion via un modem. Selon la méthode choisie (RNIS ou DSL), la connexion est contrôlée par ipppd ou par pppd. En fait, pour pouvoir se connecter, il suffit de démarrer ces programmes correctement.

Si vous possédez un forfait qui ne génère aucun coût supplémentaire pour les connexions via modem, il vous suffit simplement de démarrer le démon correspondant. Contrôlez la connexion à distance à l'aide d'une applet KDE ou d'une interface de ligne de commande. Si la passerelle Internet n'est pas l'hôte que vous utilisez, vous pouvez contrôler la connexion à distance à l'aide d'un hôte réseau.

C'est là qu'intervient smpppd. Il fournit en effet une interface uniformisée pour les programmes auxiliaires et fonctionne dans deux sens. Tout d'abord, il programme le pppd ou ipppd requis et contrôle ses propriétés de connexion. Ensuite, il permet aux programmes utilisateur d'accéder à plusieurs fournisseurs et transmet les informations relatives à l'état actuel de la connexion. Comme smpppd peut également être contrôlé à partir du réseau, il est adapté pour contrôler les connexions à Internet via modem, à partir d'un poste de travail dans un sous-réseau privé.

38.6.1 Configuration de smpppd

Les connexions fournies par smpppd sont automatiquement configurées par YaST. Les programmes de connexion proprement dits, KInternet et cinternet, sont également préconfigurés. Les paramètres manuels ne sont nécessaires que pour configurer des fonctionnalités supplémentaires de smpppd, comme le contrôle distant.

Le fichier de configuration de smpppd s'intitule `/etc/smpppd.conf`. Par défaut, il n'active pas le contrôle distant. Les principales options de ce fichier de configuration sont les suivantes :

open-inet-socket = *yes|no*
: Pour contrôler smpppd via le réseau, cette option doit avoir la valeur `yes`. Le port d'écoute de smpppd est le `3185`. Si ce paramètre est défini sur `yes`, les paramètres `bind-address`, `host-range` et `password` doivent être définis en conséquence.

bind-address = *ip*
: Si un hôte possède plusieurs adresses IP, utilisez ce paramètre pour déterminer celle sur laquelle smpppd doit accepter les connexions.

host-range = *ip min ip max*
: Le paramètre `host-range` définit une plage réseau. Ainsi, les hôtes dont les adresses IP figurent dans cette plage ont accès à smpppd. En revanche, l'accès est refusé à tous les hôtes qui ne figurent pas dans cette plage.

password = *mot de passe*
: L'assignation d'un mot de passe limite les clients aux hôtes autorisés. Comme il s'agit d'un mot de passe en clair, vous ne devez pas surestimer la sécurité qu'il procure. En l'absence de mot de passe, tous les clients ont accès à smpppd.

slp-register = *yes|no*
: Ce paramètre permet d'annoncer le service smpppd sur le réseau via SLP.

Pour plus d'informations sur smpppd, consultez les pages du manuel qui portent sur `smpppd(8)` et `smpppd.conf(5)`.

38.6.2 Configuration de KInternet, cinternet et qinternet pour une utilisation à distance

KInternet, cinternet et qinternet permettent de contrôler un smpppd local ou distant. cinternet est l'équivalent de ligne de commande de l'interface graphique KInternet. qinternet est fondamentalement identique à KInternet, à ceci près qu'il n'utilise pas les bibliothèques KDE ; il peut donc être utilisé sans KDE et doit être installé séparément. Pour préparer ces utilitaires afin de les utiliser conjointement avec un smpppd distant, modifiez le fichier de configuration `/etc/smpppd-c.conf` manuellement ou à l'aide de KInternet. Ce fichier ne comporte que trois options :

sites = *liste de sites*
: Ce paramètre permet d'indiquer aux interfaces où rechercher smpppd. Les interfaces testent les options dans l'ordre spécifié ici. L'option `local` commande l'établissement d'une connexion au smpppd local, tandis que `gateway` pointe vers un smpppd situé sur la passerelle. La connexion doit être établie conformément à la section `server` de `config-file`. `slp` ordonne aux interfaces de se connecter à un smpppd trouvé via SLP.

server = *serveur*
: Indiquez ici l'hôte sur lequel s'exécute smpppd.

password = *mot de passe*
: Insérez le mot de passe sélectionné pour smpppd.

Si smpppd est actif, vous pouvez à présent essayer d'y accéder, à l'aide de la commande `cinternet --verbose --interface-list`, par exemple. Si vous rencontrez des problèmes à ce stade, consultez les pages du manuel qui portent sur `smpppd-c.conf(5)` et `cinternet(8)`.

Services SLP sur le réseau 39

Le *protocole SLP* (Service Location Protocol - protocole de localisation de services) a été élaboré pour simplifier la configuration des clients reliés en réseau à l'intérieur d'un réseau local. Pour configurer un client réseau, avec tous les services requis, l'administrateur a généralement besoin de connaître en détail les serveurs disponibles sur le réseau. Le protocole SLP permet d'indiquer la disponibilité d'un service particulier à tous les clients du réseau local. Les applications qui prennent en charge SLP peuvent utiliser les informations diffusées et être configurées automatiquement.

SUSE Linux prend en charge l'installation à l'aide de sources d'installation fournies via SLP et contient de nombreux services système qui intègrent la prise en charge de SLP. YaST et Konqueror disposent tous deux d'interfaces client adaptées à SLP. SLP vous permet de fournir des fonctions essentielles aux clients en réseau, comme un serveur d'installation, un serveur YOU, un serveur de fichiers ou un serveur d'impression sur votre système SUSE Linux.

39.1 Enregistrement de vos propres services

Sous SUSE Linux, beaucoup d'applications disposent déjà d'une prise en charge SLP intégrée car elles utilisent la bibliothèque `libslp`. Si un service n'a pas été compilé avec prise en charge SLP, utilisez l'une des méthodes suivantes pour intégrer SLP à ce service :

Enregistrement statique via `/etc/slp.reg.d`

Créez un fichier d'enregistrement distinct pour chaque nouveau service. Voici un exemple de fichier pour l'enregistrement d'un service de scanner :

```
## Enregistrer un service « sane » sur ce système
## en désigne la langue anglaise
## 65535 désactive le timeout ; ainsi, l'enregistrement du service
## n'exige pas de rafraîchissement
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Dans ce fichier, la ligne la plus importante est l'*URL du service*, qui débute par `service:`. Elle contient le type de service (`scanner.sane`) et l'adresse à laquelle ce service est disponible sur le serveur. *`$HOSTNAME`* est automatiquement remplacé par le nom d'hôte complet. Le nom du port TCP sur lequel réside le service concerné apparaît ensuite, précédé du signe deux-points. Entrez ensuite la langue dans laquelle le service doit apparaître et la durée d'enregistrement (en secondes). Vous devez séparer ces données et l'URL du service par des virgules. La valeur indiquant la durée d'enregistrement doit être comprise entre `0` et `65535`. La valeur `0` empêche l'enregistrement. La valeur `65535` supprime toutes les restrictions.

Le fichier d'enregistrement contient également les deux variables `watch-tcp-port` et `description`. La première relie l'annonce SLP du service à l'état d'activité de ce service (slpd contrôle l'état). La deuxième variable contient une description plus précise du service, qui apparaît dans les navigateurs compatibles.

Enregistrement statique avec `/etc/slp.reg`

L'unique différence avec la procédure décrite plus haut est le regroupement de tous les services dans un seul fichier central.

Enregistrement dynamique avec slptool

Utilisez l'interface client de ligne de commande slptool si vous devez enregistrer un service pour SLP à partir de scripts propriétaires.

39.2 Interfaces client SLP dans SUSE Linux

SUSE Linux contient plusieurs interfaces client qui permettent de vérifier et d'utiliser les informations SLP à l'aide d'un réseau :

slptool
: slptool est un programme de ligne de commande simple qui permet d'annoncer des requêtes SLP sur le réseau ou d'annoncer des services propriétaires. La commande `slptool --help` répertorie toutes les fonctions et options disponibles. Vous pouvez également appeler slptool à partir de scripts qui traitent des informations SLP.

Navigateur SLP de YaST
: YaST comporte un navigateur SLP distinct qui répertorie sous forme d'arborescence tous les services du réseau local annoncés via SLP : utilisez *Services réseau → Navigateur SLP*.

Konqueror
: Utilisé comme navigateur réseau, Konqueror permet d'afficher tous les services SLP disponibles sur le réseau local (via `slp:/`). Cliquez sur les icônes de la fenêtre principale pour obtenir des informations plus détaillées sur le service correspondant. Si vous utilisez Konqueror avec `service:/`, cliquez sur l'icône correspondante une fois qu'elle apparaît dans la fenêtre du navigateur, afin de configurer une connexion avec le service sélectionné.

39.3 Activation de SLP

Si vous souhaitez proposer des services, slpd doit être exécuté sur votre système. En revanche, vous n'avez pas besoin de démarrer ce démon si vous souhaitez simplement effectuer des requêtes de service. Comme la plupart des services système sous SUSE Linux, le démon slpd est contrôlé au moyen d'un script d'initialisation distinct. Par défaut, le démon est inactif. Pour l'activer le temps d'une session, démarrez-le en exécutant `rcslpd start` en tant qu'utilisateur `root` et arrêtez-le avec `rcslpd stop`. Utilisez `restart` ou `status` pour effectuer un redémarrage ou un contrôle d'état. Si slpd doit être actif par défaut, exécutez une seule fois, en tant que `root`, la commande

insserv slpd. slpd est automatiquement intégré dans l'ensemble des services à démarrer lors de l'amorçage du système.

39.4 Pour plus d'informations

Les sources suivantes fournissent des informations complémentaires sur le protocole SLP :

RFC 2608, 2609, 2610
Le document RFC 2608 contient des généralités sur SLP. Le document RFC 2609 décrit avec plus de précision la syntaxe des URL de service utilisées et RFC 2610 traite du DHCP via SLP.

http://www.openslp.com
Page d'accueil du projet OpenSLP.

file:/usr/share/doc/packages/openslp/*
Ce répertoire contient toute la documentation disponible sur SLP, y compris le fichier README.SuSE qui contient les spécifications SUSE Linux, les documents RFC mentionnés ci-dessus et deux documents HTML de présentation. Les programmeurs qui souhaitent utiliser les fonctions SLP doivent installer le paquetage openslp-devel afin de consulter le *manuel de programmation* fourni.

40 La résolution de noms

DNS (en anglais, Domain Name System) sert à résoudre les noms de domaines et de machines, c'est-à-dire à les convertir en adresses IP. De cette manière, l'adresse IP 192.168.0.0 est par exemple attribuée au nom d'hôte `earth`.Avant de configurer votre propre serveur de noms, nous vous recommandons de consulter les informations d'ordre général relatives à la résolution de noms dans la Section 38.3, « Résolution de noms » (p. 621). Les exemples de configuration suivants font référence à BIND.

40.1 Notions de base du DNS

40.2 Configuration avec YaST

Le module DNS de YaST sert à configurer un serveur de noms dans le réseau local. Lorsque vous démarrez le module pour la première fois, un assistant apparaît et vous demande de prendre quelques décisions fondamentales sur l'administration du serveur. Une fois la configuration initiale terminée, le serveur est sommairement configuré et prêt à l'emploi dans les grandes lignes. Le mode expert sert pour des tâches de configuration plus avancées.

40.2.1 Configuration avec l'assistant

L'assistant se compose de trois étapes ou boîtes de dialogue. Vous pouvez entrer en mode expert à partir de chaque boîte de dialogue.

Configuration des redirecteurs

Lorsque ce module démarre pour la première fois, vous voyez la boîte de dialogue montrée dans la Figure 40.1, « Installation du serveur de noms : paramètres des redirecteurs » (p. 656). Décidez-y si vous souhaitez recevoir une liste des redirecteurs lorsque vous vous connectez par ADSL ou par RNIS (*Démon PPP définit les redirecteurs*), ou les lui donner vous-même (*Spécifier les redirecteurs manuellement*).

Figure 40.1 *Installation du serveur de noms : paramètres des redirecteurs*

Zones DNS

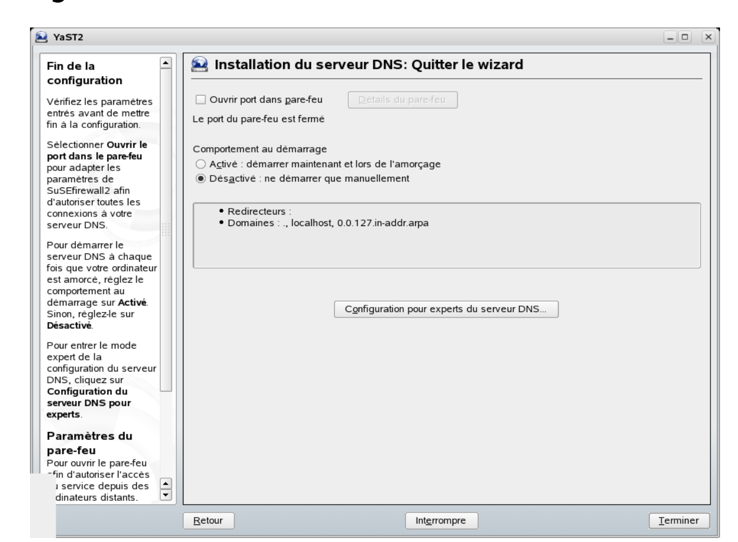
Les éléments de ce module sont expliqués dans l'installation en mode expert dans Zones DNS (p. 659). Pour créer une zone, entrez son nom dans le champ *Nom de zone*. Pour ajouter une zone inverse, faites finir le nom par `.in-addr.arpa`. Enfin, sélectionnez une valeur *Type de zone* (maître ou esclave). Consultez la Figure 40.2, « Installation d'un serveur DNS : zones DNS » (p. 657). Cliquez sur *Modifier la zone* pour configurer des paramètres supplémentaires pour une zone existante. Pour supprimer une zone, cliquez sur *Supprimer la zone*.

Figure 40.2 *Installation d'un serveur DNS : zones DNS*

Terminer avec l'assistant

Dans la dernière boîte de dialogue, vous pouvez ouvrir le port DNS (port `53`) dans le pare-feu activé pendant l'installation et décider si le DNS doit être démarré. Vous pouvez également accéder à la configuration en mode expert depuis cette boîte de dialogue. Reportez-vous à la Figure 40.3, « Installation du serveur de noms : terminer avec l'assistant » (p. 658).

Figure 40.3 Installation du serveur de noms : terminer avec l'assistant



40.2.2 Configuration avancée

Lorsque le module démarre pour la première fois, YaST ouvre une fenêtre offrant plusieurs possibilités de configuration. Dès que la configuration est terminée, le serveur de noms est en principe prêt à fonctionner :

Démarrage

Dans la section *Amorçage*, vous pouvez définir si le serveur DNS doit être démarré en même temps que le système (lors de l'amorçage) ou manuellement. Les boutons *Démarrer le serveur DNS maintenant* et *Arrêter le serveur DNS maintenant* permettent respectivement de démarrer et d'arrêter le serveur de noms immédiatement. *Enregistrer les paramètres et redémarrer le serveur DNS maintenant* vous permet d'enregistrer la configuration actuelle. Vous pouvez ouvrir le port DNS du pare-feu (*Ouvrir port dans pare-feu*) et modifier l'installation du pare-feu dans *Paramètres du pare-feu*.

Redirecteurs

Cette boîte de dialogue est identique à celle qui apparaît au démarrage de l'assistant de configuration (voir Configuration des redirecteurs (p. 656)).

Journalisation

Cette rubrique vous servira à paramétrer ce que le serveur de noms doit consigner dans son journal et comment. Précisez dans *Type de journal* l'endroit où le serveur de noms doit consigner ses messages. Vous pouvez utiliser le fichier de journal global du système `/var/log/messages` en choisissant *Journaliser dans le journal système* ou spécifier un autre fichier en choisissant *Journaliser dans le fichier*. Dans ce cas, définissez aussi la taille maximale du fichier en méga-octets et le nombre de fichiers journaux à garder.

Journalisations additionnelles vous permet d'ajuster d'autres options. *Journaliser toutes les requêtes DNS* enregistre *chaque* requête. Le fichier journal peut donc devenir très volumineux rapidement. Vous ne devriez choisir cette option qu'à des fins de débogage. Pour consigner le flux de données lors des mises à jour de zones entre le serveur DHCP et le serveur DNS, choisissez l'option*Journaliser les mises à jour de zone*. Pour consigner le flux de données lors des transferts de zones du maître vers l'esclave, activez l'option *Journaliser les transferts de zone* . Reportez-vous à la Figure 40.4, « Serveur DNS : journalisation » (p. 659).

Figure 40.4 *Serveur DNS : journalisation*

Zones DNS

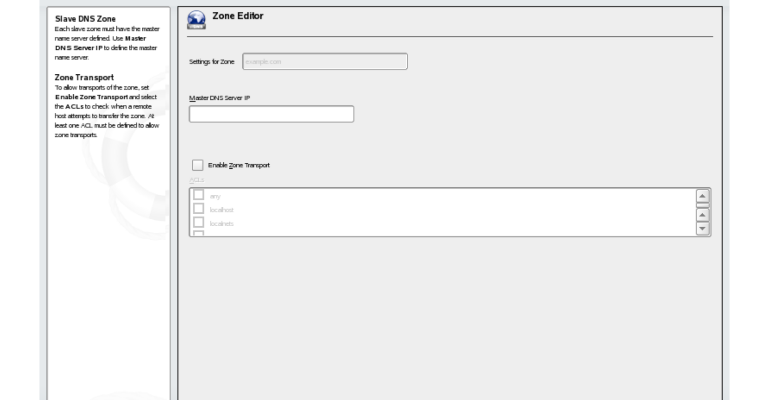
Cette boîte de dialogue est divisée en plusieurs parties et permet de gérer des fichiers de zones (voir la Section 40.5, « Fichiers de zone » (p. 669)). Dans *Nom de zone* saisissez le nom d'une nouvelle zone. Pour créer des zones inverses, le nom de la

zone doit se terminer par `.in-addr.arpa`. Choisissez le type (maître ou esclave) avec *Type de zone*. Le bouton *Modifier zone...* vous permet de modifier d'autres réglages. Lorsque vous voulez supprimer une zone, cliquez sur *Effacer zone*.

Éditeur de zones esclaves

Cette boîte de dialogue apparaît si vous avez choisi à l'étape décrite dans Zones DNS (p. 659) *Esclave* comme type de zone. Indiquez dans le champ *Serveur DNS maître* le serveur maître duquel l'esclave doit obtenir ses données. Si vous souhaitez limiter l'accès au serveur, choisissez une des ACL définies au préalable dans la liste. Reportez-vous à la Figure 40.5, « Serveur DNS : éditeur de zones esclaves » (p. 660).

Figure 40.5 *Serveur DNS : éditeur de zones esclaves*



Éditeur de zones maîtres

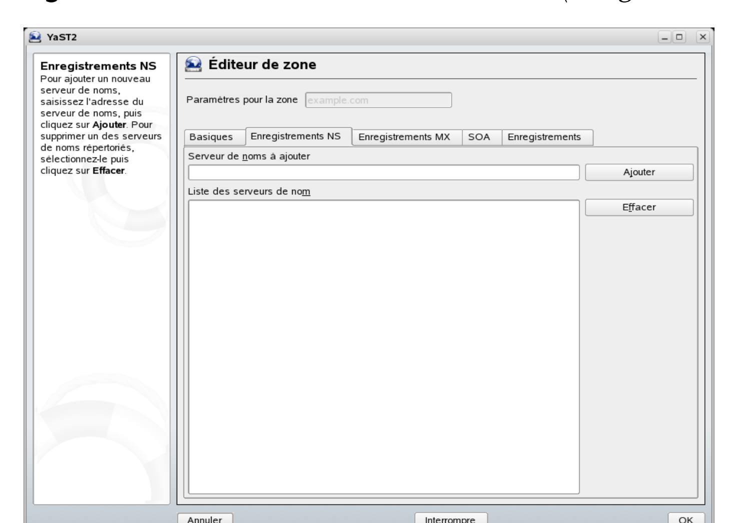
Cette boîte de dialogue apparaît si vous avez choisi à l'étape décrite dans Zones DNS (p. 659) *Maître* comme type de zone. Elle se subdivise en plusieurs vues : *Basiques* (la première page ouverte), *Enregistrements NS*, *Enregistrements MX*, *SOA* et *Enregistrements*.

Éditeur de zones (enregistrements NS)

Cette boîte de dialogue permet de définir un serveur de noms secondaire pour ces zones. Veillez à ce que le serveur de nom proprement dit soit contenu dans la liste. Pour saisir un nouvel enregistrement, indiquez dans *Serveur de nom à ajouter* le

nom correspondant et confirmez au moyen de *Ajouter*. Reportez-vous à la Figure 40.6, « Serveur DNS : éditeur de zones (enregistrements NS) » (p. 661).

Figure 40.6 *Serveur DNS : éditeur de zones (enregistrements NS)*



Éditeur de zones (enregistrements MX)

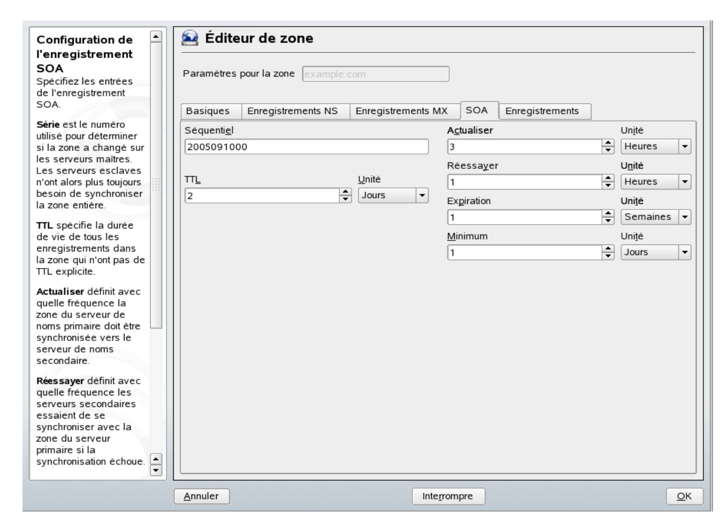
Pour ajouter un nouveau serveur de messagerie pour la zone actuelle à la liste en place, indiquez l'adresse et la valeur de priorité voulues. Confirmez au moyen de *Ajouter*. Reportez-vous à la Figure 40.7, « Serveur DNS : éditeur de zones (enregistrements MX) » (p. 662)).

Figure 40.7 *Serveur DNS : éditeur de zones (enregistrements MX)*

Éditeur de zones (SOA)

Cette page vous permet de créer des enregistrements SOA (*Start of Authority*). L'Exemple 40.6, « Fichier /var/lib/named/monde.zone » (p. 670) explique les différentes options.

Figure 40.8 *Serveur DNS : éditeur de zones (SOA)*



Éditeur de zones (enregistrements)

Cette boîte de dialogue vous permet de gérer une liste d'affectations de noms à des adresses IP. Indiquez dans la zone de saisie *Nom* le nom d'hôte puis choisissez son type. *A-Record* représente l'enregistrement principal. *CNAME* est un alias. Dans *MX-Relay*, l'enregistrement (Nom) est remplacé par la valeur (Valeur).

40.3 Démarrer le serveur de noms BIND

Le serveur de noms BIND (*Berkeley Internet Name Domain*) est déjà configuré dans SUSE Linux de manière à ce que vous puissiez le démarrer tout de suite après avoir effectué l'installation. Lorsque vous avez déjà une connexion Internet qui fonctionne et que vous indiquez dans le fichier `/etc/resolv.conf` le serveur de noms `127.0.0.1` pour `localhost`, vous possédez déjà, en règle générale, une résolution de noms fonctionnant parfaitement sans connaître le DNS du fournisseur d'accès. BIND effectue alors la résolution de noms par l'intermédiaire du serveur de noms racine, ce qui est en revanche beaucoup plus lent. On devra normalement indiquer le DNS du fournisseur d'accès ainsi que son adresse IP dans le fichier de configuration `/etc/named.conf` dans la rubrique `forwarders` pour bénéficier d'une résolution de noms efficace et sûre. Tant que cela fonctionne, le serveur de noms fonctionne en tant que serveur de noms « cache seulement » (caching-only). Ce n'est que lorsque l'on mettra à sa disposition ses propres zones qu'il deviendra un véritable serveur de noms. Vous en trouverez un exemple simple dans le répertoire de documentation `/usr/share/doc/packages/bind/sample-config`.

ASTUCE: Adaptation automatique des déclarations de serveurs de noms

Les déclarations des serveurs de noms peuvent être adaptées automatiquement à la situation, en fonction de la façon d'accéder à Internet ou de l'environnement réseau. Pour cela, positionnez la variable `MODIFY_NAMED_CONF_DYNAMICALLY` du fichier `/etc/sysconfig/network/config` à la valeur `yes`.

Il ne faut cependant pas définir un nom de domaine officiel sans l'avoir fait au préalable approuver par l'institution compétente. Même lorsque vous disposez de votre propre domaine et qu'il est géré par votre fournisseur d'accès, nous vous recommandons de ne pas l'utiliser dans la mesure où BIND ne redirigerait plus aucune requête pour ce

domaine. Le serveur Web du fournisseur d'accès dédié à votre propre domaine ne pourrait par exemple plus être joint.

Pour démarrer le serveur de noms, saisissez en tant que `root` la commande `rcnamed start`. Si « done » apparaît en vert à droite, named, c'est-à-dire le processus du serveur de noms, est démarré avec succès. Vous pouvez tester immédiatement sur le système local le fonctionnement du serveur de noms avec les programmes `host` ou `dig` qui devraient renvoyer `localhost` comme serveur par défaut avec l'adresse `127.0.0.1`. Si tel n'était pas le cas, cela signifierait qu'un mauvais nom de serveur figure probablement dans le fichier `/etc/resolv.conf` ou que ce fichier n'existe tout simplement pas. Testez pour commencer `host 127.0.0.1`, qui devrait normalement toujours fonctionner. Si vous obtenez un message d'erreur, utilisez la commande `rcnamed status` pour vérifier que le processus `named` a bien été lancé. Si le serveur de noms ne démarre pas ou se comporte de manière inattendue, vous en trouverez normalement la cause dans le fichier `/var/log/messages`.

Pour utiliser en tant que redirecteur (forwarder) le serveur de noms du fournisseur d'accès ou un de vos propres serveurs de noms déjà en service sur votre réseau local, il faut indiquer la ou les adresses IP correspondantes dans la section `options` avec le mot-clé `forwarders`. Les adresses IP utilisées dans l'Exemple 40.1, « Options de redirection (forwarding) dans named.conf » (p. 664) sont choisies de manière arbitraire et doivent être adaptées à vos propres besoins.

Exemple 40.1 *Options de redirection (forwarding) dans named.conf*

```
options {
    directory "/var/lib/named";
 forwarders { 10.11.12.13; 10.11.12.14; };
 listen-on { 127.0.0.1; 192.168.0.99; };
 allow-query { 127/8; 192.168.0/24; };
 notify no;
 };
```

Après les `options` viennent les déclarations de zones, `localhost` et`0.0.127.in-addr.arpa`. L'enregistrement `type hint` situé sous « . » doit toujours être présent. Les fichiers correspondants ne doivent pas être modifiés et ils devraient fonctionner en l'état. Vous devez veiller également à ce que chaque ligne soit suivie d'un **;** et que les accolades soient placées correctement. Si vous avez entrepris des modifications dans le fichier de configuration `/etc/named.conf` ou dans les fichiers des zones, vous devez ordonner à BIND de les lire à nouveau à l'aide de la commande `rcnamed reload`. Vous pouvez arriver au même résultat en redémarrant

complètement le serveur de noms avec la commande `rcnamed restart`. Vous pouvez arrêter à tout moment le serveur de noms avec la commande `rcnamed stop`.

40.4 Le fichier de configuration /etc/named.conf

Tous les paramétrages du serveur de noms BIND sont enregistrés dans le fichier `/etc/named.conf`. Les données de zone, les noms des machines, les adresses IP, etc. des domaines à gérer sontenregistrées dans des fichiers séparés du répertoire `/var/lib/named`. Vous trouverez davantage d'informations à ce sujet plus loin.

Le fichier `/etc/named.conf` se divise principalement en deux parties : d'une part, la section `options` pour les paramètres d'ordre général et, d'autre part, les déclarations de `zone` des différents domaines. La section `logging` (journalisation) et les déclarations d'`acl` (contrôle d'accès) sont optionnelles. Les lignes de commentaires commencent par le signe dièse `#` ou par une barre de division `//`. L'Exemple 40.2, « Fichier /etc/named.conf minimaliste » (p. 665) présente un fichier `/etc/named.conf` minimaliste.

Exemple 40.2 *Fichier /etc/named.conf minimaliste*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1;};
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

40.4.1 Les options de configuration importantes

directory "*nom*"

indique le répertoire dans lequel BIND trouve les fichiers contenant les données de zones. Il s'agit en général de `/var/lib/named`.

forwarders { *adresse-ip*; };

indique les serveurs de noms (la plupart du temps ceux du fournisseur d'accès) vers lesquels on redirige les requêtes DNS auxquelles il n'est pas possible de répondre directement. À la place d'*adresse-ip* vous devez mettre une adresse IP comme `10.0.0.1`.

forward first;

a pour effet que les requêtes DNS sont redirigées avant même que le serveur de noms racine n'essaie de les résoudre. Vous pouvez utiliser `forward only` à la place de `forward first` pour que toutes les requêtes soient redirigées et que le serveur de noms racine ne soit plus du tout consulté. Cela peut se révéler utile pour la configuration des pare-feu.

listen-on port 53 { 127.0.0.1; *adresse-ip*; };

indique à BIND sur quelles interfaces réseau et sur quel port il doit écouter les requêtes des clients. Vous n'êtes pas obligé de saisir `53` dans la mesure où 53 est de toute façon le port par défaut. `127.0.0.1` permet d'accepter les requêtes de la machine locale. Si vous omettez complètement cette ligne, par défaut toutes les interfaces sont utilisées.

listen-on-v6 port 53 { any; };

indique à BIND sur quel port il doit écouter les requêtes des clients qui utilisent IPv6. Outre `any`, seul `none` est également autorisé car le serveur écoute toujours l'adresse joker IPv6.

query-source address * port 53;

Cette directive peut être utile lorsqu'un pare-feu bloque les requêtes DNS externes. Cela oblige BIND à effectuer ses requêtes vers l'extérieur à partir du port 53 et pas des ports supérieurs à 1024.

query-source-v6 address * port 53;
Cette directive doit être utilisée pour les requêtes basées sur IPv6.

allow-query { 127.0.0.1; *réseau*; };
précise les réseaux à partir desquels les clients ont le droit d'envoyer des requêtes DNS. Il faut mettre à la place de *réseau* une adresse de la forme `192.168.1/24` où `/24` est un raccourci pour le nombre de bits dans le masque réseau, soit dans ce cas `255.255.255.0`.

allow-transfer { ! *; };
détermine quels ordinateurs sont autorisés à effectuer des transferts de zone. Cet exemple les interdit complètement du fait de la présence de `! *`. Sans cette directive, il est possible de réaliser des transferts de zone sans aucune limitation et depuis n'importe où.

statistics-interval 0;
Sans cette directive, BIND produit toutes les heures plusieurs lignes de messages de statistiques dans `/var/log/messages`. Paramétrez-la à `0` pour les supprimer complètement ou spécifiez un intervalle en minutes.

cleaning-interval 720;
Cette option définit au bout de quel intervalle BIND vide son cache. Cette action est à chaque fois consignée dans un enregistrement du fichier `/var/log/messages`. Le temps est indiqué ici en minutes. La valeur par défaut est de 60 minutes.

interface-interval 0;
BIND parcourt régulièrement les interfaces réseau pour détecter de nouvelles interfaces ou celles qui ne sont plus disponibles. Réglez cette valeur à `0` pour l'en empêcher et pour que BIND n'écoute que les interfaces trouvées au démarrage. Vous pouvez aussi préciser l'intervalle en minutes. La valeur par défaut est de 60 minutes.

notify no;
Le `no` signifie qu'aucun autre serveur de noms n'est averti en cas de modifications apportées aux données de zone ou lors du redémarrage du serveur de noms.

40.4.2 journalisation

BIND vous permet de configurer complètement ce qui est consigné dans un journal, comment et à quel endroit. Les paramétrages par défaut sont normalement suffisants. L'Exemple 40.3, « La journalisation est désactivée » (p. 668) montre la forme la plus simple d'une telle directive et permet d'empêcher complètement la journalisation.

Exemple 40.3 *La journalisation est désactivée*

```
logging {
        category default { null; };
};
```

40.4.3 Déclarations de zones

Exemple 40.4 *Déclaration de zone pour mon-domaine.fr*

```
zone "mon-domaine.fr" in {
       type master;
       file "mon-domaine.zone";
       notify no;
};
```

Après le mot-clé `zone`, on indique le nom du domaine géré (`mon-domaine.fr`), suivi de `in` puis, entre accolades, d'un bloc d'options qui s'appliquent à ce domaine comme le montre l'Exemple 40.4, « Déclaration de zone pour mon-domaine.fr » (p. 668). Si vous souhaitez définir une *zone esclave* (slave), changez la valeur du `type` en `slave` et indiquez un serveur de noms qui gère cette zone en tant que `maître` (master) (qui peut à son tour être l'esclave d'un autre maître) comme le montre l'Exemple 40.5, « Déclaration de zone pour autre-domaine.fr » (p. 668).

Exemple 40.5 *Déclaration de zone pour autre-domaine.fr*

```
zone "autre-domaine.fr" in {
       type slave;
       file "slave/autre-domaine.zone";
       masters { 10.0.0.1; };
};
```

Les options de zones :

type master;
Le mot-clé `master` indique que cette zone est gérée par ce serveur de noms. Cela suppose que l'on dispose d'un fichier de zone correct.

type slave;
Cette zone est transférée depuis un autre serveur de noms. Elle doit être utilisée en conjonction avec des serveurs maîtres.

type hint;
La zone `.` de type `hint` est utilisée pour indiquer le serveur de noms racine. Vous pouvez laisser cette définition de zone telle quelle.

file "mon-domaine.zone" ou file "slave/autre-domaine.zone";
Cette déclaration indique le fichier dans lequel figurent les données de zone du domaine. Dans le cas d'un esclave, ce fichier n'est pas nécessaire car son contenu est récupéré sur un autre serveur de noms. Pour bien distinguer les fichiers maîtres des fichiers esclaves, on place les fichiers esclaves dans le répertoire `slave`.

masters { *adresse-ip-du-serveur*; };
Cette directive n'est utile que pour les zones esclaves et elle indique depuis quel serveur de noms le fichier de zones doit être transféré.

allow-update { ! *; };
Cette option régit l'accès en écriture depuis l'extérieur, ce qui permettrait à des clients de s'inscrire eux-mêmes dans le DNS — ce qui, pour des raisons de sécurité, n'est normalement pas souhaitable. Lorsque cette directive n'est pas présente, les mises à jour des zones ne sont pas autorisées du tout. Dans cet exemple, cela ne changerait rien non plus dans la mesure où `! *` interdit également toute action de ce type.

40.5 Fichiers de zone

Deux types de fichiers de zones sont nécessaires. Le premier sert à associer l'adresse IP au nom de l'ordinateur. L'autre fonctionne en sens inverse et fournit un nom d'hôte pour une adresse IP donnée.

ASTUCE: Point (.) dans les fichiers de zones

Le . a une signification importante dans le fichier de zones. Si vous indiquez les noms des ordinateurs sans . final, la zone ajoutée à la fin. Il est donc important de terminer les noms d'ordinateurs complets par un . final, pour que le domaine n'y soit pas encore ajouté. Un point oublié ou mal placé est probablement la cause la plus fréquente d'erreur dans la configuration des serveurs de noms.

Considérons, tout d'abord, le fichier de zone `monde.zone`, responsable du domaine `monde.entier`, montré dans l'Exemple 40.6, « Fichier /var/lib/named/monde.zone » (p. 670).

***Exemple 40.6** Fichier /var/lib/named/monde.zone*

```
$TTL 2D
monde.entier.   IN SOA      gateway  root.monde.entier. (
            2003072441  ; serial
            1D          ; refresh
            2H          ; retry
            1W          ; expiry
            2D )        ; minimum

            IN NS       gateway
            IN MX       10 soleil

gateway     IN A        192.168.0.1
            IN A        192.168.1.1
soleil      IN A        192.168.0.2
lune        IN A        192.168.0.3
terre       IN A        192.168.1.2
mars        IN A        192.168.1.3
www         IN CNAME    lune
```

Ligne 1 :
`$TTL` définit la durée de vie par défaut (en anglais, Time To Live), c'est-à-dire la durée de vie valable de toutes les directives de ce fichier : 2 jours (2D = 2 days).

Ligne 2 :
C'est ici que commence l'`enregistrement de contrôle SOA` (SOA = Start of Authority) :

- En première position, on trouve le nom du domaine à gérer `monde.entier`, ce dernier se terminant par un . car sinon la zone serait à nouveau ajoutée. Sinon,

on peut aussi écrire ici un `@` pour que la zone de la directive correspondante soit extraite du fichier `/etc/named.conf`.

- Après `IN SOA`, on trouve le nom du serveur de noms qui sert de maître pour cette zone. Dans ce cas, le nom `gateway` est complété pour devenir `gateway.monde.entier` car il ne se termine pas par un `.`.

- Vient ensuite l'adresse électronique de la personne responsable du serveur de noms. Comme le signe `@` a déjà une signification particulière, il faut simplement écrire un `.` à la place. Ainsi, pour `root@monde.entier`, on écrit `root.monde.entier.`. N'oubliez pas le `.` à la fin, sans quoi la zone serait à nouveau ajoutée.

- Vient enfin une parenthèse `(` qui permet d'englober les lignes qui suivent jusqu'à la parenthèse `)` dans l'enregistrement SOA.

Ligne 3 :

Le `numéro de série` est un nombre arbitraire qui doit être incrémenté à chaque modification de ce fichier. Il sert à informer les serveurs de noms secondaires (serveurs esclaves) des modifications entreprises. On a donc introduit pour ce faire un nombre à 10 chiffres composé de la date et d'un numéro d'ordre de la forme `AAAAMMJJNN`.

Ligne 4 :

La `fréquence d'actualisation` indique à quels intervalles le serveur de noms secondaire vérifie le `numéro de série` de la zone. Dans cet exemple, on a pris 1 jour (1D = 1 day).

Ligne 5 :

La `fréquence des tentatives` indique l'écart de temps qui s'écoule avant qu'un serveur de noms secondaire, en cas d'erreur, n'essaie de contacter à nouveau le serveur principal. Dans le cas présent, on a 2 heures (2H = 2 hours).

Ligne 6 :

La `durée d'expiration` indique la durée au bout de laquelle un serveur de noms secondaire jette les données mises en cache s'il n'a plus réussi à contacter le serveur principal. Dans le cas présent, il s'agit d'une semaine (1W = 1 week).

Ligne 7 :
La dernière ligne du SOA est la `durée de vie de mise en cache des échecs`. Elle indique combien de temps les résultats des requêtes DNS des autres serveurs qui n'ont pu être résolues peuvent être conservées en mémoire cache.

Ligne 9 :
`IN NS` indique le serveur de noms responsable de ce domaine. Ici aussi, le nom `gateway` est complété pour devenir `gateway.monde.entier` car il ne se termine pas par un `.`. On peut utiliser plusieurs lignes de ce type, une pour le serveur principal et une pour chaque serveur de noms secondaire. Si `notify` dans le fichier `/etc/named.conf` ne vaut pas `no`, tous les serveurs de noms indiqués ici sont informés des modifications des données de la zone.

Ligne :10 :
L'enregistrement MX indique le serveur de messagerie qui prend en charge, modifie et redirige les messages pour le domaine `monde.entier`. Dans cet exemple, il s'agit de l'ordinateur `soleil.monde.entier`. Le chiffre qui précède le nom de l'ordinateur est la valeur de préférence. Ainsi, s'il existe plusieurs déclarations MX, c'est le serveur de messagerie dont la valeur de préférence est la plus petite qui est pris, et si la remise de courrier à ce serveur échoue, on essaie celui ayant la valeur plus élevée suivante.

Lignes 12 à 17 :
Il s'agit là des véritables enregistrements d'adresses (en anglais, address records), dans lesquels on attribue une ou plusieurs adresses IP à un nom d'ordinateur. Les noms figurent ici sans `.` final, car ils sont indiqués sans domaine à leur suite et sont donc tous complétés par `monde.entier`. Deux adresses IP sont attribuées à l'ordinateur `gateway` car il est équipé de deux cartes réseau. Le `A` indique une adresse de machine traditionnelle ; on utilise `A6` pour les adresses IPv6 (`AAAA` est un format dépassé pour les adresses IPv6).

Ligne 18 :
On peut utiliser l'alias `www` pour désigner `lune` (`CNAME` = `canonical name`, nom canonique).

Pour la résolution inverse (en anglais, reverse lookup) des adresses IP en noms de machines, on utilise le pseudo-domaine `in-addr.arpa`. Ce dernier est ajouté à l'adresse réseau écrite dans l'ordre inverse. `192.168.1` devient donc `1.168.192.in-addr.arpa`. Reportez-vous à l'Exemple 40.7, « Résolution inverse » (p. 673).

Exemple 40.7 *Résolution inverse*

```
$TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.monde.entier. root.monde.entier. (
      2003072441      ; serial
      1D              ; refresh
      2H              ; retry
      1W              ; expiry
      2D )            ; minimum

      IN NS           gateway.monde.entier.

1                       IN PTR          gateway.monde.entier.
2                       IN PTR          terre.monde.entier.
3                       IN PTR          mars.monde.entier.
```

Ligne 1 :
$TTL définit la durée de vie par défaut valable ici pour toutes les directives.

Ligne 2 :
Ce fichier permet en principe la résolution inverse pour le réseau `192.168.1.0`. Comme la zone s'appelle ici `1.168.192.in-addr.arpa`, on ne souhaite bien entendu pas l'ajouter au nom d'hôte. C'est pourquoi on saisit ce dernier en entier—avec le domaine et le `.` final. Le reste correspond à ce qui a déjà été décrit dans l'exemple précédent pour la zone `monde.entier`.

Lignes 3 à 7 :
Voir l'exemple précédent pour `monde.entier`.

Ligne 9 :
Cette ligne indique ici aussi à nouveau le serveur de noms responsable de cette zone, mais cette fois-ci, le nom est indiqué en entier, avec le domaine et le `.` final.

Lignes 11 à 13 :
Il s'agit d'enregistrements pointeurs (pointer records) qui, pour une adresse IP pointent vers le nom d'ordinateur correspondant. On trouve au début de cette ligne uniquement le dernier chiffre de l'adresse IP, sans `.` final. Si l'on y ajoute la zone et que l'on fait abstraction de `.in-addr.arpa`, on obtient bien l'adresse IP complète en ordre inversé.

Les transferts de zones entre différentes versions de BIND ne doivent, normalement, pas poser de problème.

40.6 Actualisation dynamique des données de zones

La mise à jour dynamique (en anglais, dynamic update) est le terme technique qui décrit l'ajout, la modification et la suppression de directives dans les fichiers de zones d'un serveur maître. Ce mécanisme est décrit dans le document RFC 2136. Les mises à jour dynamiques se configurent, par zone, à l'aide des options `allow-update` ou `update-policy` au niveau des déclarations des zones. Vous ne devez pas modifier manuellement les zones mises à jour de manière dynamique.

La commande `nsupdate` sert à transmettre au serveur les enregistrements à mettre à jour. Pour connaître sa syntaxe exacte, reportez-vous à la page de manuel de `nsupdate` (`man 8 nsupdate`). Pour des raisons de sécurité, la mise à jour doit impérativement s'effectuer au moyen de transactions sécurisées (TSIG) comme décrit dans la Section 40.7, « Transactions sécurisées » (p. 674).

40.7 Transactions sécurisées

On peut effectuer des transactions sécurisées avec les « signatures de transactions » (TSIG, transaction SIGnatures). On utilise, pour ce faire, des clés de transaction (en anglais, transaction keys) et des signatures de transaction (en anglais, transaction signatures). La section suivante explique comment les générer et les utiliser.

Les transactions sécurisées sont nécessaires dans le cadre de la communication d'un serveur à un autre et pour l'actualisation dynamique des données de zones. Un contrôle d'accès fondé sur des clés permet d'obtenir un niveau de sécurité bien plus élevé qu'un contrôle fondé sur les adresses IP.

Vous pouvez générer une clé de transaction avec la commande suivante (pour plus d'informations, cf. la page de manuel relative à la commande `dnssec-keygen`) :

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Cette commande génère deux fichiers portant, par exemple, les noms suivants :

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

La clé (par exemple `ejIkuCyyGJwwuN3xAteKgg==`) est contenue dans les deux fichiers. Pour une utilisation ultérieure, `Khost1-host2.+157+34265.key` doit être transmis, de préférence par un chemin sécurisé à l'ordinateur distant (par exemple avec `scp`). La clé doit être ajoutée dans le fichier `/etc/named.conf` de l'hôte distant pour établir une communication sécurisée entre `host1` et `host2` :

```
key host1-host2. {
  algorithm hmac-md5;
  secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

AVERTISSEMENT: Droits d'accès de `/etc/named.conf`

Veillez à ce que les droits d'accès au fichier `/etc/named.conf` restent restreints. La valeur par défaut est `0640` pour `root` et le groupe `named`. Vous pouvez aussi stocker la clé dans un fichier protégé indépendant pour l'inclure ensuite dans le fichier `/etc/named.conf`.

Pour que la clé pour `host2` soit utilisée sur le serveur `host1` avec, par exemple, l'adresse `192.168.2.3`, il faut saisir, sur le serveur, dans le fichier `/etc/named.conf`, les informations suivantes :

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

Il faut aussi saisir des directives similaires dans les fichiers de configuration de `host2`.

Pour effectuer des transactions sécurisées, il faut, en plus des ACL (listes de contrôle d'accès, à ne pas confondre avec les ACL du système de fichiers) basées sur les adresses et les intervalles d'adresses IP, ajouter des clés TSIG. L'enregistrement correspondant peut se présenter ainsi :

```
allow-update { key host1-host2. ;};
```

Pour en savoir plus, consultez le *Manuel de référence de l'administrateur BIND* sous `update-policy`.

40.8 Sécurité de DNS

DNSSEC (en anglais, DNS Security, sécurité de DNS) est décrite dans le document RFC 2535. Le manuel de BIND décrit les outils disponibles permettant d'utiliser DNSSEC.

Une zone sûre doit posséder une ou plusieurs clés de zones. Utilisez la commande `dnssec-keygen` pour les générer, à l'instar des clés d'hôte. On utilise actuellement DSA pour générer les clés. Les clés publiques doivent être intégrées dans le fichier de zone correspondant avec une directive `$INCLUDE`.

Toutes les clés sont regroupées en un ensemble à l'aide de la commande `dnssec-makekeyset`, lequel doit être acheminé jusqu'à la zone parent (parent zone) par un chemin sûr pour y être signé à l'aide de la commande `dnssec-signkey`. Les fichiers générés lors de cette signature doivent être utilisés pour signer les zones avec la commande `dnssec-signzone` et les fichiers en résultant doivent finalement être intégrés au fichier `/etc/named.conf` pour chaque zone.

40.9 Informations supplémentaires

Nous vous recommandons notamment de consulter le *Manuel de référence de l'administrateur BIND* que vous trouverez en ligne dans `/usr/share/doc/packages/bind/`, ainsi que les RFC mentionnés dans ce dernier et les pages de manuel fournies avec BIND. Vous trouverez des informations à jour concernant la configuration de BIND sous SUSE Linux dans `/usr/share/doc/packages/bind/README.SuSE`.

Utilisation de NIS 41

Dès que plusieurs systèmes UNIX d'un réseau veulent accéder à des ressources communes, il est essentiel que toutes les identités des groupes et des utilisateurs soient identiques sur toutes les machines du réseau. Le réseau doit être transparent pour les utilisateurs : quelle que soit la machine utilisée, ils doivent toujours se retrouver dans le même environnement. Ceci est possible grâce aux services NIS et NFS. Le service NFS, qui distribue les systèmes de fichiers sur le réseau, est traité dans le Chapitre 42, *Partage des systèmes de fichiers avec NFS* (p. 685).

Le NIS (Network Information Service - service d'informations réseau) est un service de base de données qui fournit un accès au contenu des fichiers `/etc/passwd`, `/etc/shadow` et `/etc/group` sur les réseaux. Vous pouvez également utiliser NIS pour d'autres tâches (par exemple, pour rendre disponible le contenu des fichiers `/etc/hosts` ou `/etc/services`), mais ces fonctions ne sont pas abordées dans cette introduction. On utilise souvent *YP* comme synonyme de NIS, puisqu'il joue le rôle de « pages jaunes » (« yellow pages » en anglais) du réseau.

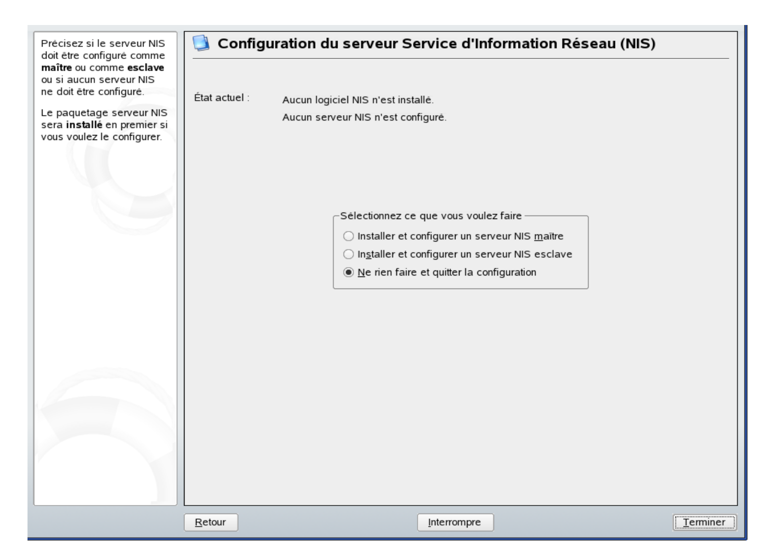
41.1 Configuration des serveurs NIS à l'aide de YaST

Pour configurer NIS, sélectionnez *Serveurs NIS* dans le module YaST *Services réseau*. Si votre réseau ne comporte pas encore de serveur NIS, activez l'option *Installer et configurer un serveur NIS maître* dans l'écran suivant. YaST installe immédiatement les paquetages nécessaires.

Si vous avez déjà installé le logiciel NIS, cliquez sur *Créer un serveur NIS maître*. Si vous disposez déjà d'un serveur NIS (*maître*), vous pouvez ajouter un serveur NIS esclave (par exemple, pour configurer un nouveau sous-réseau). Examinons tout d'abord la configuration du serveur maître. Si vous cliquez sur *Ne rien faire et quitter la configuration*, vous revenez au centre de contrôle YaST sans enregistrer les modifications.

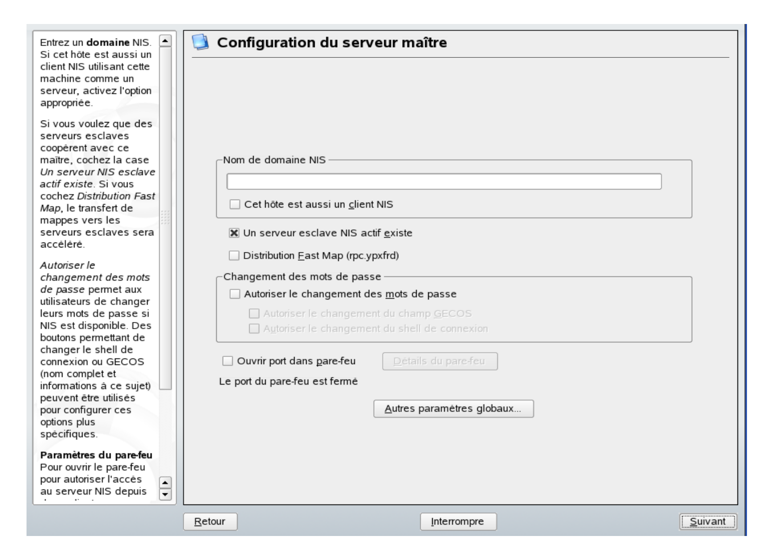


Figure 41.1 *Configuration du serveur NIS*



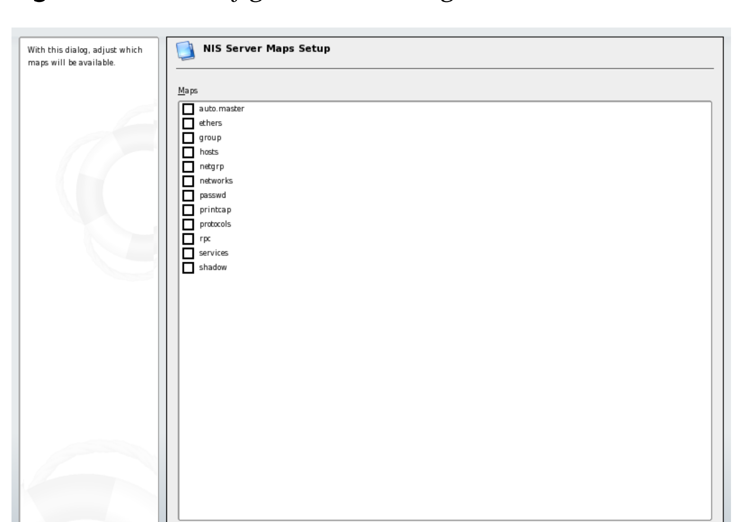
Une fois tous les paquetages installés, saisissez le nom de domaine NIS en haut de la boîte de dialogue de configuration représentée à la Figure 41.1, « Configuration du serveur NIS » (p. 678). Si vous souhaitez que l'hôte soit également un client NIS, cochez la case correspondante pour permettre aux utilisateurs de se loguer et d'accéder aux données à partir du serveur NIS. Cochez les options que vous souhaitez activer, y compris dans la section *Changement des mots de passe*. Pour définir d'autres options, cliquez sur *Autres paramètres globaux*. Vous accédez ainsi à un écran où vous pouvez modifier le répertoire source, fusionner des mots de passe et définir les plus petits ID de groupe et d'utilisateur. Cliquez sur *OK* pour revenir à la boîte de dialogue principale. Cliquez sur *Suivant* pour poursuivre la configuration.

Figure 41.2 *Configuration du serveur maître*



Dans l'écran suivant, indiquez les assignations à rendre disponibles. Cliquez sur *Suivant* pour accéder à l'écran suivant, qui vous permet de déterminer les hôtes autorisés à interroger le serveur NIS. Vous pouvez ajouter, supprimer et modifier des hôtes. Cliquez sur *Terminer* pour enregistrer les modifications et quitter la boîte de dialogue de configuration.

Figure 41.3 Configuration des assignations du serveur NIS



Pour configurer d'autres serveurs NIS (*esclaves*) sur votre réseau, activez maintenant l'option *Installer et configurer un serveur NIS esclave*. Si vous avez déjà installé le logiciel NIS, sélectionnez *Créer un serveur NIS esclave*, puis cliquez sur *Suivant* pour continuer. Dans l'écran suivant, saisissez le nom de domaine NIS et cochez les cases appropriées.

Pour autoriser les utilisateurs de votre réseau (les utilisateurs locaux et ceux qui sont administrés par le serveur NIS) à modifier leur mot de passe sur le serveur NIS (à l'aide de la commande `yppasswd`), activez l'option correspondante. Les options *Autoriser le changement du champ GECOS* et *Autoriser le changement du shell de connexion* sont alors disponibles. « GECOS » signifie que les utilisateurs peuvent aussi modifier leurs paramètres de nom et d'adresse à l'aide de la commande `ypchfn`. « SHELL » permet aux utilisateurs de modifier leur shell par défaut à l'aide de la commande `ypchsh`, par exemple, pour passer de bash à sh.

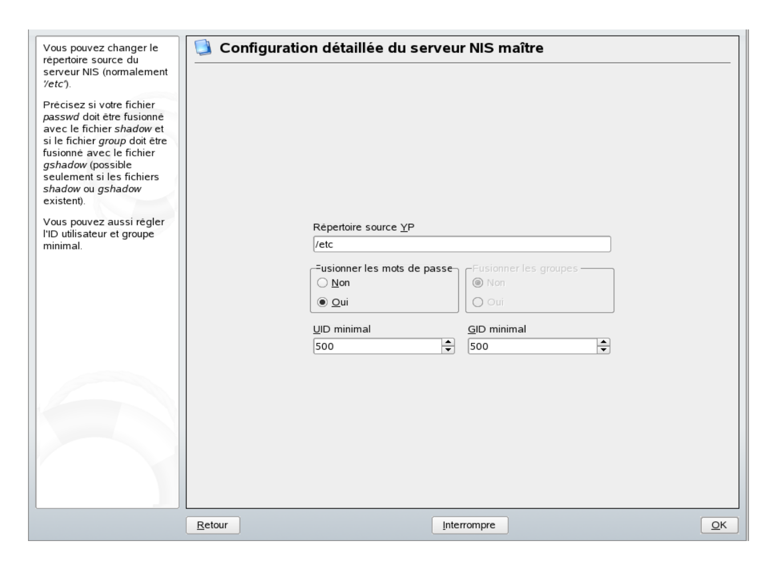
Pour définir d'autres options, cliquez sur *Autres paramètres globaux*. L'écran auquel vous accédez, représenté par la Figure 41.4, « Changement de répertoire et synchronisation des fichiers pour un serveur NIS » (p. 681), vous permet de modifier le répertoire source du serveur NIS (par défaut, `/etc`). Il vous permet également de fusionner des mots de passe et des groupes. Vous devez sélectionner *Oui* pour que les fichiers `/etc/passwd`, `/etc/shadow` et `/etc/group` puissent être synchronisés.

Vous pouvez également déterminer les plus petits ID d'utilisateur et de groupe. Cliquez sur *OK* pour confirmer le paramétrage et revenir à l'écran précédent.

Une fois les paramètres sélectionnés, cliquez sur *Suivant* pour accéder à l'écran suivant. Dans la boîte de dialogue suivante, consultez les assignations qui seront disponibles, puis cliquez sur *Suivant* pour continuer. Dans le dernier écran, indiquez les hôtes autorisés à interroger le serveur NIS. Pour ajouter, modifier ou supprimer des hôtes, cliquez sur les boutons correspondants. Cliquez sur *Terminer* pour enregistrer les modifications et quitter la configuration.

Ensuite, cliquez sur *Suivant*.

***Figure 41.4** Changement de répertoire et synchronisation des fichiers pour un serveur NIS*



Si vous avez précédemment activé l'option *Un serveur esclave NIS actif existe*, saisissez les noms d'hôte utilisés comme esclaves, puis cliquez sur *Suivant*. Si vous n'utilisez pas de serveurs esclaves, la configuration esclave est ignorée et vous accédez directement à la boîte de dialogue de configuration de la base de données. Indiquez ici les *assignations*, c'est-à-dire les bases de données partielles à transférer du serveur NIS au client. Les paramètres par défaut sont généralement appropriés.

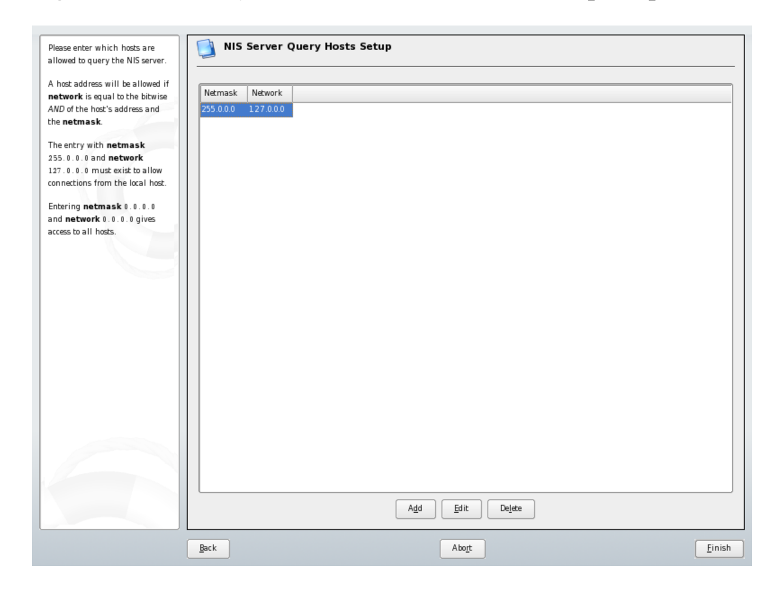
Cliquez sur *Suivant* pour accéder à la dernière boîte de dialogue, représentée par la Figure 41.5, « Définition des autorisations de requête pour un serveur NIS » (p. 682).

Indiquez les réseaux à partir desquels les requêtes peuvent être envoyées au serveur NIS. En règle générale, il s'agit de votre réseau interne. Dans ce cas, les deux entrées suivantes doivent apparaître :

```
255.0.0.0     127.0.0.0
0.0.0.0       0.0.0.0
```

La première entrée active les connexions à partir de votre propre hôte, le serveur NIS. La deuxième autorise tous les hôtes qui disposent d'un accès au même réseau à envoyer des requêtes au serveur.

Figure 41.5 *Définition des autorisations de requête pour un serveur NIS*



IMPORTANT: Configuration automatique du pare-feu

Si un pare-feu est actif sur votre système (SUSEfirewall2), YaST adapte sa configuration au serveur NIS en activant le service `portmap` lorsque vous sélectionnez *Ouvrir port dans pare-feu*.

41.2 Configuration des clients NIS

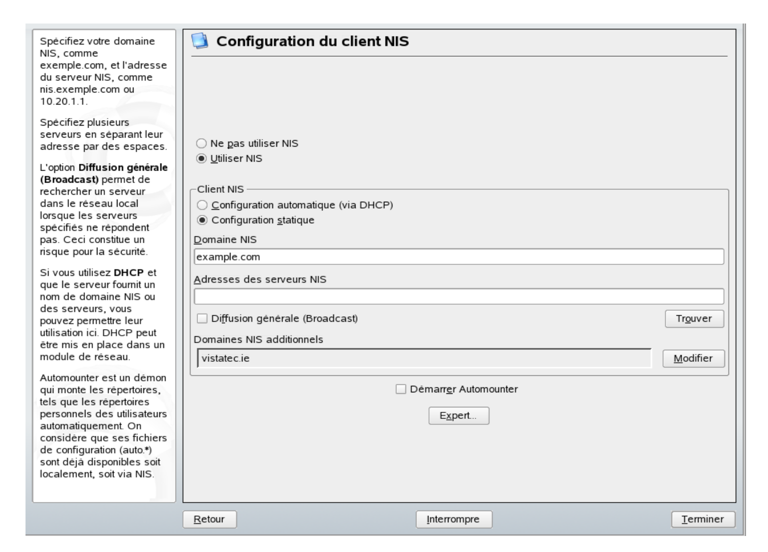
Ce module permet de configurer un client NIS. Après avoir choisi d'utiliser NIS et éventuellement, le monteur automatique, cette boîte de dialogue apparaît. Indiquez si l'hôte dispose d'une adresse IP statique ou s'il en reçoit une émise par le protocole DHCP. DHCP fournit également le domaine et le serveur NIS. Pour plus d'informations sur DHCP, consultez le Chapitre 43, *DHCP* (p. 691). Si une adresse IP statique est utilisée, indiquez manuellement le domaine et le serveur NIS. (voir Figure 41.6, « Définition du domaine et de l'adresse d'un serveur NIS » (p. 684)). Si vous activez l'option *Trouver*, YaST recherche un serveur NIS actif sur votre réseau. L'option *Diffusion générale (Broadcast)* active la recherche dans le réseau local afin de trouver un serveur si les serveurs spécifiés ne répondent pas.

Pour indiquer plusieurs serveurs, vous pouvez saisir leurs adresses dans le champ *Adresses des serveurs NIS*, en les séparant par des espaces.

En mode de configuration pour experts, désactivez l'option *Répondre aux hôtes distants* si vous ne souhaitez pas que d'autres hôtes puissent interroger le serveur utilisé par votre client. Activez l'option *Serveur défectueux* pour permettre au client de recevoir des réponses en provenance d'un serveur qui communique via un port non privilégié. Pour plus d'informations, consultez la commande `man ypbind`.

Une fois le paramétrage terminé, cliquez sur *Terminer* pour appliquer les modifications et revenir au centre de contrôle YaST.

Figure 41.6 *Définition du domaine et de l'adresse d'un serveur NIS*



Partage des systèmes de fichiers avec NFS

42

Comme l'indique le Chapitre 41, *Utilisation de NIS* (p. 677), NFS fonctionne en parallèle avec NIS pour rendre le réseau transparent pour l'utilisateur. NFS permet de distribuer des systèmes de fichiers sur le réseau. Peu importe le terminal auquel les utilisateurs sont connectés, ils doivent toujours se retrouver dans le même environnement.

Tout comme NIS, NFS est un service asymétrique. Il existe des serveurs NFS et des clients NFS. Une même machine peut remplir les deux rôles : elle peut fournir des systèmes de fichiers sur le réseau (exportation) et monter des systèmes de fichiers à partir d'autres hôtes (importation). Il s'agit généralement de serveurs dotés d'une grande capacité de disque dur, dont les systèmes de fichiers sont montés par d'autres clients.

IMPORTANT: Nécessité d'un DNS

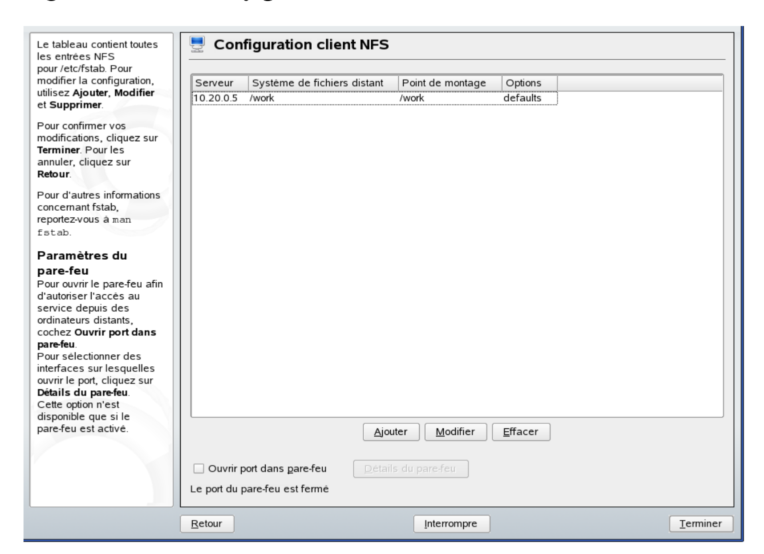
En principe, toutes les exportations peuvent s'effectuer à l'aide des seules adresses IP. Toutefois, il est préférable de disposer d'un système DNS en fonctionnement pour éviter les timeouts. C'est notamment nécessaire pour des raisons de journalisation, puisque le démon mountd effectue des recherches inverses.

42.1 Importation de systèmes de fichiers avec YaST

Les utilisateurs qui y sont autorisés peuvent monter des répertoires NFS dans leurs propres arborescences de fichiers, à partir d'un serveur NFS. Pour ce faire, le moyen le

plus simple consiste à utiliser le module *Client NFS* de YaST. Saisissez le nom d'hôte du serveur NFS, le répertoire à importer et le point de montage de ce répertoire au niveau local. Cliquez ensuite sur *Ajouter* dans la première boîte de dialogue. Cliquez sur *Ouvrir port dans pare-feu* pour ouvrir le pare-feu, afin d'autoriser les ordinateurs distants à accéder au service. L'état du pare-feu apparaît en regard de la case à cocher. Cliquez sur *OK* pour enregistrer les modifications. (voir Figure 42.1, « Configuration du client NFS avec YaST » (p. 686)).

Figure 42.1 *Configuration du client NFS avec YaST*



42.2 Importation manuelle des systèmes de fichiers

Vous pouvez facilement importer des systèmes de fichiers depuis un serveur NFS. Il suffit que le portmapper RPC soit en service. Pour le démarrer, entrez la commande `rcportmap start` en tant qu'utilisateur `root`. Lorsque cette condition préalable est remplie, vous pouvez monter des systèmes de fichiers distants, exportés depuis les machines correspondantes, dans le système de fichiers à l'aide de la commande `mount`comme s'il s'agissait de disques locaux. La syntaxe est la suivante :

```
mount hôte:chemin distant chemin local
```

Ainsi, la commande pour importer les répertoires personnels de la machine sun est la suivante :

```
mount sun:/home /home
```

42.3 Exportation de systèmes de fichiers avec YaST

YaST vous permet de transformer un hôte de votre réseau en serveur NFS, c'est-à-dire un serveur qui exporte des répertoires et des fichiers vers tous les hôtes autorisés à y accéder. Des applications peuvent ainsi être mises à la disposition de tous les membres d'un groupe, sans être installées localement sur chacun des hôtes. Pour installer ce type de serveur, démarrez YaST, puis sélectionnez *Services réseau* → *Serveur NFS*. Une boîte de dialogue semblable à celle de la Figure 42.2, « Outil de configuration du serveur NFS » (p. 687) apparaît.

Figure 42.2 *Outil de configuration du serveur NFS*

Ensuite, activez l'option *Démarrer le serveur NFS*, puis cliquez sur *Suivant*. Dans le champ supérieur, indiquez les répertoires à exporter. En dessous, indiquez les hôtes que vous voulez voir accéder à ces répertoires. Cette boîte de dialogue apparaît dans la Figure 42.3, « Configuration d'un serveur NFS avec YaST » (p. 688). Vous pouvez

définir quatre options pour chaque hôte : `single host`, `netgroups`, `wildcards` et `IP networks`. Pour en savoir plus sur ces options, consultez la commande `man exports`. Pour terminer la configuration, cliquez sur *Quitter*.

Figure 42.3 *Configuration d'un serveur NFS avec YaST*

IMPORTANT: Configuration automatique du pare-feu

Si un pare-feu est actif sur votre système (SUSEfirewall2), YaST adapte sa configuration pour le serveur NFS en activant le service `nfs` lorsque vous sélectionnez *Ouvrir port dans pare-feu*.

42.4 Exportation manuelle des systèmes de fichiers

Si vous ne souhaitez pas utiliser YaST, vous devez vous assurer que les services suivants sont activés sur le serveur NFS :

- Portmapper RPC (portmap)
- Démon RPC de montage (rpc.mountd)

- Démon RPC NFS (rpc.nfsd)

Pour permettre aux scripts /etc/init.d/portmap et /etc/init.d/nfsserver de lancer ces services lors du démarrage du système, saisissez les commandes insserv /etc/init.d/nfsserver et insserv /etc/init.d/portmap. Indiquez ensuite quels systèmes de fichiers doivent être exportés et vers quel hôte. Ces éléments sont définis dans le fichier de configuration /etc/exports.

Pour chaque répertoire à exporter, une ligne est nécessaire pour déterminer les machines autorisées à accéder à ce répertoire ainsi que les autorisations connexes. Tous les sous-répertoires de ce répertoire sont également exportés automatiquement. Les machines autorisées sont généralement spécifiées avec leur nom complet (y compris le nom de domaine), mais vous pouvez utiliser des caractères joker, comme l'astérisque (*) ou le point d'interrogation (?), qui fonctionnent de la même manière que dans le shell Bash. Si aucun nom de machine n'est indiqué, toutes les machines sont autorisées à importer ce système de fichiers avec les autorisations indiquées.

Indiquez entre parenthèses, après le nom de la machine, les autorisations du système de fichiers à exporter. Les principales options apparaissent dans le Tableau 42.1, « Autorisations liées au système de fichiers exporté » (p. 689).

***Tableau 42.1** Autorisations liées au système de fichiers exporté*

Option	Signification
ro	Le système de fichiers est exporté avec une autorisation en lecture seule (valeur par défaut).
rw	Le système de fichiers est exporté avec une autorisation en lecture/écriture.
root_squash	Cette option garantit que l'utilisateur root d'une machine qui importe des données ne dispose d'aucune autorisation racine (root) sur ce système de fichiers. Pour cela, vous devez assigner l'ID utilisateur 65534 aux utilisateurs dont l'ID est 0 (root). Cet ID utilisateur doit être défini sur nobody (valeur par défaut).

Option	Signification
no_root_squash	N'assigne pas l'ID utilisateur 0 à l'utilisateur dont l'ID est 65534. Les autorisations racine (root) restent donc valides.
link_relative	Convertit les liens absolus (qui commencent par /) en une suite de ../. Cette option n'est utile que si le système de fichiers d'une machine a été intégralement monté (valeur par défaut).
link_absolute	Les liens symboliques restent intacts.
map_identity	Les ID utilisateur sont exactement identiques sur le client et le serveur (valeur par défaut).
map_daemon	Le client et le serveur utilisent des ID utilisateur distincts. Cette option conduit nfsd à créer une table de conversion des ID utilisateur. Le démon ugidd est nécessaire au bon fonctionnement de cette option.

Votre fichier exports doit ressembler à celui de l'Exemple 42.1, « /etc/exports » (p. 690). Le fichier /etc/exports est lu par mountd et nfsd. Si vous apportez des modifications à ce fichier, redémarrez mountd et nfsd pour qu'elles soient appliquées. Pour ce faire, le plus simple est d'exécuter la commande rcnfsserver restart.

Exemple 42.1 */etc/exports*

```
#
# /etc/exports
#
/home               sun(rw)    venus(rw)
/usr/X11            sun(ro)    venus(ro)
/usr/lib/texmf      sun(ro)    venus(rw)
/                   earth(ro,root_squash)
/home/ftp           (ro)
# End of exports
```

43 DHCP

L'objectif du *protocole de configuration dynamique d'hôtes DHCP* (Dynamic Host Configuration Protocol) est d'assigner des paramètres réseau de façon centralisée à partir d'un serveur plutôt que de les configurer localement sur chaque poste de travail. Un hôte configuré pour utiliser DHCP ne peut pas contrôler sa propre adresse statique. Il se configure lui-même totalement et automatiquement en fonction des indications fournies par le serveur.

L'une des utilisations du protocole DHCP consiste à identifier chaque client à l'aide de l'adresse matérielle de sa carte réseau (qui est généralement fixe), puis de fournir des paramètres identiques à ce client chaque fois qu'il se connecte au serveur. Vous pouvez également configurer le protocole DHCP de façon à ce que le serveur assigne dynamiquement des adresses à chaque client intéressé, à partir d'un ensemble d'adresses configuré dans ce but. Dans ce cas, le serveur DHCP s'efforce d'assigner la même adresse au client à chaque fois qu'il reçoit une requête de sa part, même au bout de longues périodes. Bien entendu, cela fonctionne uniquement tant que le réseau ne dispose pas de plus de clients que d'adresses.

Grâce à ces différentes possibilités, le protocole DHCP peut faciliter la vie des administrateurs système de deux façons. Toutes les modifications, même les plus importantes, relatives aux adresses et à la configuration réseau en général peuvent être mises en œuvre de façon centralisée en modifiant le fichier de configuration du serveur. Cette procédure est bien plus pratique que la reconfiguration de plusieurs postes de travail. En outre, il est beaucoup plus facile d'intégrer des ordinateurs, et notamment de nouveaux postes, dans le réseau, puisque vous pouvez leur attribuer une adresse IP issue de l'ensemble. La récupération des paramètres réseau appropriés à partir d'un serveur DHCP s'avère particulièrement utile dans le cas d'ordinateurs portables régulièrement utilisés dans différents réseaux.

Un serveur DHCP fournit l'adresse IP et le masque réseau mais également le nom d'hôte, le nom de domaine, la passerelle et les adresses du serveur de noms que le client doit utiliser. En outre, le protocole DHCP permet de configurer d'autres paramètres de façon centralisée. Il peut s'agir, par exemple, d'un serveur horaire, à partir duquel les clients peuvent demander l'heure actuelle, ou même d'un serveur d'impression.

43.1 Configuration d'un serveur DHCP avec YaST

Lorsque vous démarrez le module pour la première fois, un assistant vous demande de prendre quelques décisions simples concernant l'administration du serveur. L'exécution de ce paramétrage initial génère une configuration serveur basique prête à fonctionner. Vous pouvez utiliser le mode expert pour effectuer des tâches de configuration plus pointues.

Sélection de la carte

Lors de la première étape, YaST recherche les interfaces réseau disponibles sur votre système, puis les affiche sous forme de liste. Dans cette liste, sélectionnez l'interface sur laquelle le serveur DHCP doit écouter. Cliquez sur *Ajouter*, puis sélectionnez *Ouvrir le pare-feu pour l'interface sélectionnée* pour ouvrir le pare-feu sur cette interface. (voir Figure 43.1, « Serveur DHCP : Sélection de la carte » (p. 693)).

Figure 43.1 Serveur DHCP : Sélection de la carte

Paramètres globaux

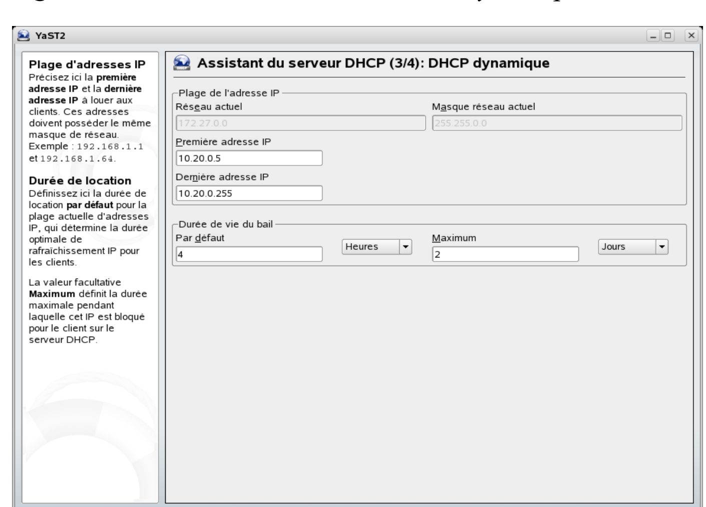
Dans les champs de saisie, indiquez les détails du réseau pour tous les clients que le serveur DHCP doit gérer. Ces informations sont le nom de domaine, l'adresse d'un serveur horaire, les adresses des serveurs de noms primaire et secondaire, les adresses d'un serveur d'impression et d'un serveur WINS (pour un réseau mixte avec des clients Windows et des clients Linux), l'adresse de la passerelle et la durée du bail. (voir Figure 43.2, « Serveur DHCP : Paramètres globaux » (p. 694)).

Figure 43.2 Serveur DHCP : Paramètres globaux

DHCP dynamique

Lors de cette étape, vous déterminez comment les adresses IP dynamiques doivent être assignées aux clients. Pour ce faire, spécifiez une plage IP à partir de laquelle le serveur peut assigner des adresses aux clients DHCP. Toutes ces adresses doivent être couvertes par le même masque réseau. Indiquez également la durée du bail pendant laquelle un client peut conserver son adresse IP sans devoir demander un prolongement du bail. Si vous le souhaitez, vous pouvez indiquer la durée de bail maximale, c'est-à-dire la période pendant laquelle le serveur réserve une adresse IP à un client spécifique. (voir Figure 43.3, « Serveur DHCP : DHCP dynamique » (p. 695)).

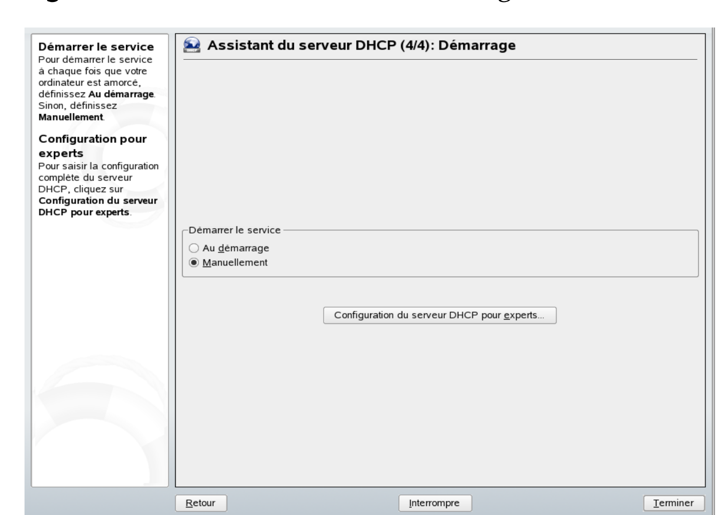
Figure 43.3 *Serveur DHCP : DHCP dynamique*



Fin de la configuration et choix du mode de démarrage

Une fois la troisième étape de l'assistant de configuration terminée, une dernière boîte de dialogue vous invite à définir le mode de démarrage du serveur DHCP. Indiquez ici si vous souhaitez que le serveur DHCP démarre automatiquement lors du démarrage du système ou si vous souhaitez le lancer manuellement lorsque cela est nécessaire (pour le tester, par exemple). Cliquez sur *Terminer* pour achever la configuration du serveur. (voir Figure 43.4, « Serveur DHCP : Démarrage » (p. 696)).

Figure 43.4 *Serveur DHCP : Démarrage*



43.2 Paquetages logiciels DHCP

SUSE Linux comprend à la fois un serveur et des clients DHCP. Le serveur DHCP disponible, dhcpd, est publié par l'ISC, Internet Software Consortium. Côté client, choisissez entre deux programmes client DHCP : dhclient (provenant également de l'ISC) et le démon client DHCP du paquetage `dhcpcd`.

SUSE Linux installe dhcpcd par défaut. Ce programme est très facile à gérer et se lance automatiquement à chaque démarrage du système pour rechercher un serveur DHCP. Il ne nécessite aucun fichier de configuration pour faire son travail et est prêt à fonctionner dans la plupart des configurations standard. Dans les situations plus complexes, utilisez le programme dhclient d'ISC, qui est contrôlé à l'aide du fichier de configuration `/etc/dhclient.conf`.

43.3 Le démon dhcpd du serveur DHCP

L'élément central de tout système DHCP est le démon de protocole de configuration dynamique d'hôtes. Ce serveur *loue* des adresses et observe leur utilisation, en fonction des paramètres définis dans le fichier de configuration `/etc/dhcpd.conf`. Pour influencer le comportement du programme de différentes façons, l'administrateur système peut modifier les paramètres et les valeurs de ce fichier. Vous trouverez une illustration simple de fichier `/etc/dhcpd.conf` dans l'Exemple 43.1, « Le fichier de configuration /etc/dhcpd.conf » (p. 697).

***Exemple 43.1** Le fichier de configuration /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2 heures

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
   range 192.168.1.10 192.168.1.20;
   range 192.168.1.100 192.168.1.200;
 }
```

Ce fichier de configuration simple est suffisant pour permettre au serveur DHCP d'assigner des adresses IP dans le réseau. Assurez-vous qu'un point-virgule est inséré à la fin de chaque ligne. Si ce n'est pas le cas, dhcpd ne démarre pas.

L'exemple de fichier ci-dessus peut être divisé en trois sections. La première détermine la durée du bail par défaut (en secondes) d'une adresse IP louée à un client demandeur (`default-lease-time`). Une fois ce délai écoulé, il doit demander un renouvellement. Cette section contient également une indication de la période maximale pendant laquelle une machine peut conserver une adresse IP assignée par le serveur DHCP sans demander de renouvellement (`max-lease-time`).

Dans la deuxième partie, des paramètres réseau de base sont définis au niveau global :

- La ligne `option domain-name` définit le domaine par défaut de votre réseau.

- L'entrée `option domain-name-servers` vous permet de spécifier jusqu'à trois valeurs correspondant aux serveurs DNS utilisés pour la résolution des adresses IP en noms d'hôte et inversement. L'idéal est de configurer un serveur de noms sur votre machine ou ailleurs sur votre réseau avant de configurer DHCP. Ce serveur de noms doit également définir un nom d'hôte pour chaque adresse dynamique et inversement. Pour savoir comment configurer votre propre serveur de noms, consultez le Chapitre 40, *La résolution de noms* (p. 655).

- La ligne `option broadcast-address` définit l'adresse de diffusion que le client demandeur doit utiliser.

- `option routers` permet d'indiquer au serveur où envoyer les paquets de données qui ne peuvent pas être fournis à un hôte sur le réseau local (selon l'adresse de l'hôte source et cible et le masque de sous-réseau fourni). Généralement, et notamment dans les réseaux de plus petite taille, ce routeur est identique à la passerelle Internet.

- `option subnet-mask` vous permet d'indiquer le masque réseau assigné aux clients.

La dernière section du fichier permet de définir un réseau, y compris un masque de sous-réseau. Pour terminer, indiquez la plage d'adresses que le démon DHCP doit utiliser pour assigner des adresses IP aux clients intéressés. Dans cet exemple, les clients peuvent utiliser toutes les adresses comprises entre `192.168.1.10` et `192.168.1.20` et entre `192.168.1.100` et `192.168.1.200`.

Après avoir modifié ces quelques lignes, vous êtes en mesure d'activer le démon DHCP à l'aide de la commande `rcdhcpd start`. Il est prêt à être utilisé immédiatement. Utilisez la commande `rcdhcpd check-syntax` pour effectuer une rapide vérification de la syntaxe. En cas de problème inattendu concernant votre configuration (le serveur est interrompu et indique une erreur ou ne retourne pas le message `done` au démarrage), vous trouverez la cause du dysfonctionnement dans le journal système principal (`/var/log/messages`) ou sur la console numéro 10 (Ctrl + Alt + F10).

Dans un système SUSE Linux par défaut, le démon DHCP est démarré dans un environnement chroot pour des raisons de sécurité. Vous devez copier les fichiers de configuration dans l'environnement chroot pour que le démon puisse les trouver. En fait, vous n'avez généralement rien à faire puisque la commande `rcdhcpd start` copie automatiquement les fichiers.

43.3.1 Clients avec adresses IP fixes

Comme indiqué précédemment, le protocole DHCP permet également d'assigner une adresse statique prédéfinie à un client spécifique pour chaque requête. Les adresses assignées explicitement sont toujours prioritaires sur les adresses dynamiques issues de l'ensemble. En outre, une adresse statique n'arrive jamais à expiration, contrairement à une adresse dynamique. C'est le cas par exemple lorsqu'il n'y a pas assez d'adresses disponibles et que le serveur doit les redistribuer aux clients.

Pour identifier un client configuré avec une adresse *statique*, dhcpd utilise l'adresse matérielle. Il s'agit d'un numéro fixe et unique sur le réseau, composé de six paires d'octets pour l'identification de tous les périphériques réseau (par exemple, `00:00:45:12:EE:F4`). Si les lignes correspondantes, comme celles de l'Exemple 43.2, « Ajouts au fichier de configuration » (p. 699), sont ajoutées au fichier de configuration de l'Exemple 43.1, « Le fichier de configuration /etc/dhcpd.conf » (p. 697), le démon DHCP assigne toujours le même ensemble de données au client correspondant dans toutes les circonstances.

Exemple 43.2 *Ajouts au fichier de configuration*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

Le nom du client respectif (`host` *`nom d'hôte`*, ici `earth`) apparaît sur la première ligne et l'adresse MAC apparaît sur la suivante. Sur les hôtes Linux, cette adresse peut être déterminée par la commande `ifstatus` suivie du périphérique réseau (par exemple, `eth0`). Si nécessaire, activez d'abord la carte réseau à l'aide de la commande `ifup eth0`. Vous obtenez alors un résultat semblable à :

```
link/ether 00:00:45:12:EE:F4
```

Dans l'exemple précédent, l'adresse IP `192.168.1.21` et le nom d'hôte earth sont assignés automatiquement au client dont la carte réseau possède l'adresse MAC `00:00:45:12:EE:F4`. Le type de matériel à saisir est `ethernet` dans la plupart des cas, même si `token-ring`, que l'on trouve fréquemment sur les systèmes IBM, est également pris en charge.

43.3.2 La version SUSE Linux

Pour améliorer la sécurité, la version SUSE du serveur DHCP d'ISC contient le correctif non-root/chroot d'Ari Edelkind. Cela permet d'exécuter dhcpd avec l'ID utilisateur `nobody` dans un environnement chroot (`/var/lib/dhcp`). Pour que cela soit possible, le fichier de configuration `dhcpd.conf` doit être situé dans `/var/lib/dhcp/etc`. Au démarrage, le script d'initialisation copie automatiquement le fichier dans ce répertoire.

Pour contrôler le comportement du serveur concernant cette fonction, utilisez les entrées du fichier `/etc/sysconfig/dhcpd`. Pour exécuter dhcpd sans l'environnement chroot, définissez la variable `DHCPD_RUN_CHROOTED` de `/etc/sysconfig/dhcpd` sur « no ».

Pour permettre à dhcpd de résoudre les noms d'hôte, y compris à partir de l'environnement chroot, vous devez également copier d'autres fichiers de configuration :

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Ces fichiers sont copiés dans `/var/lib/dhcp/etc/` au démarrage du script d'initialisation. Tenez compte de ces copies pour toute modification qu'elles requièrent si elles sont modifiées de manière dynamique par des scripts tels que `/etc/ppp/ip-up`. Toutefois, vous n'avez pas à vous en inquiéter si le fichier de configuration indique uniquement des adresses IP (et pas de noms d'hôte).

Si votre configuration comporte des fichiers supplémentaires qui doivent être copiés dans l'environnement chroot, indiquez-les sous la variable `DHCPD_CONF_INCLUDE_FILES` dans le fichier `/etc/sysconfig/dhcpd`. Pour vous assurer que la fonction de journalisation de DHCP continue à fonctionner après un redémarrage du démon syslog, vous devez ajouter l'option `-a /var/lib/dhcp/dev/log` sous `SYSLOGD_PARAMS` dans le fichier `/etc/sysconfig/syslog`.

43.4 Pour plus d'informations

Pour plus d'informations sur le protocole DHCP, consultez le site Web de l'*Internet Software Consortium* (`http://www.isc.org/products/DHCP/`). Vous pouvez également consulter les pages du manuel sur `dhcpd`, `dhcpd.conf`, `dhcpd.leases` et `dhcp-options`.

Synchronisation avec xntp 44

Le mécanisme NTP (network time protocol) est un protocole de synchronisation de l'heure système sur le réseau. La machine peut tout d'abord obtenir l'heure à partir d'un serveur qui est une source de temps fiable. Une machine peut ensuite agir elle-même en tant que source de l'heure pour d'autres ordinateurs du réseau. L'objectif est double : maintenir le temps absolu et synchroniser l'heure système de toutes les machines d'un réseau.

La conservation d'une heure système exacte est importante dans de nombreuses situations. L'horloge matérielle (BIOS) intégrée ne correspond souvent pas aux exigences d'applications telles que les bases de données. La correction manuelle de l'heure système se traduirait par de graves problèmes. En effet, un saut en arrière peut par exemple provoquer le dysfonctionnement d'applications critiques. Sur un réseau, il est généralement nécessaire de synchroniser l'heure système de toutes les machines, mais le réglage manuel de l'heure est une mauvaise approche. xntp fournit un mécanisme permettant de résoudre ces problèmes. Il règle en continu l'heure système à l'aide des serveurs de temps du réseau. Il permet en outre la gestion d'horloges de référence locales, telles que des horloges contrôlées par radio.

44.1 Configuration d'un client NTP avec YaST

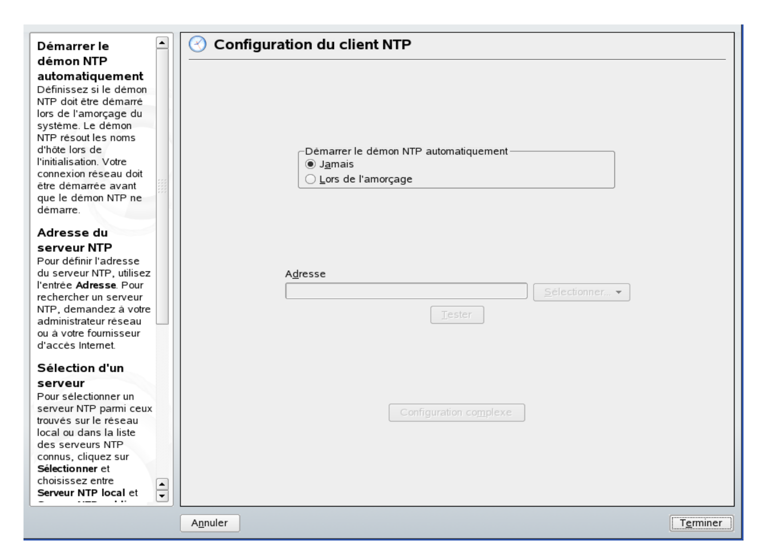
xntp est prédéfini pour utiliser l'horloge de l'ordinateur local comme référence de temps. L'utilisation de l'horloge (BIOS), cependant, ne sert que comme recours si aucune source de temps d'une précision supérieure n'est disponible. SUSE Linux facilite la configuration

d'un client NTP avec YaST. Vous pouvez utiliser la configuration rapide ou la configuration complexe pour les clients qui n'exécutent pas SuSEfirewall. Ces clients font en effet partie d'un intranet protégé. Les deux sont décrites ci-dessous.

44.1.1 Configuration rapide du client NTP

La configuration rapide du client NTP (*Services réseau* → *Client NTP*) comporte deux boîtes de dialogue. Vous définissez le mode de démarrage de xntpd et le serveur à interroger dans la première boîte de dialogue. Pour démarrer xntpd automatiquement lors de l'amorçage du système, cliquez sur *Lors de l'amorçage*. Cliquez ensuite sur *Sélectionner* pour accéder à une seconde boîte de dialogue dans laquelle vous pouvez sélectionner un serveur de temps pour votre réseau.

***Figure 44.1** YaST : configuration d'un client NTP*



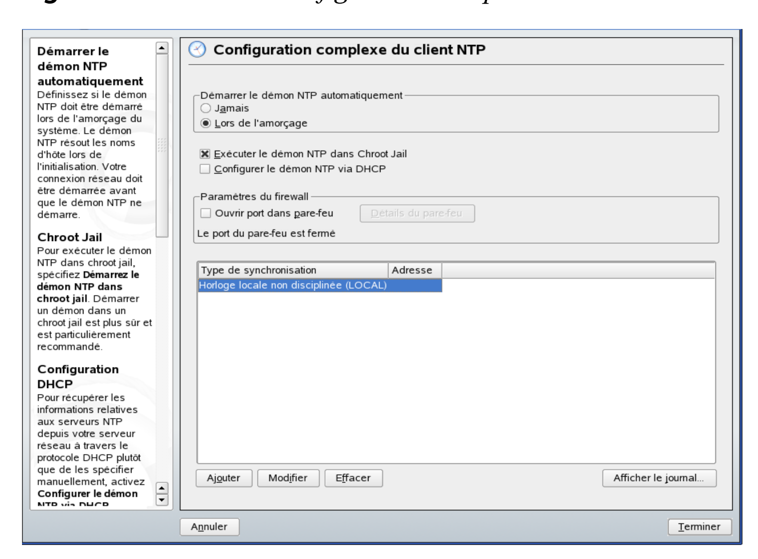
Dans la boîte de dialogue détaillée de sélection du serveur, déterminez si la synchronisation doit être implémentée en utilisant un serveur de temps de votre réseau local (*Serveur local NTP*) ou un serveur de temps basé sur Internet qui gère votre fuseau horaire (*Serveur NTP public*). Pour un serveur de temps local, cliquez sur *Recherche* pour démarrer une requête SLP et trouver les serveurs de temps disponibles sur votre réseau. Sélectionnez le serveur de temps le mieux adapté dans la liste des résultats de recherche et quittez la boîte de dialogue en cliquant sur *OK*. Pour un serveur NTP public, sélectionnez votre pays (fuseau horaire) ainsi que le serveur approprié dans la liste

située sous *Serveur NTP public* et quittez la boîte de dialogue en cliquant sur *OK*. Dans la boîte de dialogue principale, testez la disponibilité du serveur sélectionné en cliquant sur *Test* et quittez la boîte de dialogue en cliquant sur *Terminer*.

44.1.2 configuration complexe du client NTP

La configuration complexe d'un client NTP est accessible sous *Configuration complexe* dans la boîte de dialogue principale du module *Client NTP*, illustrée dans Figure 44.1, « YaST : configuration d'un client NTP » (p. 704), après avoir sélectionné le mode de démarrage comme indiqué dans la configuration rapide.

Figure 44.2 *YaST : configuration complexe du client NTP*



Dans *Configuration complexe du client NTP*, déterminez si xntpd doit être démarré dans un chroot jail. Ceci augmente la sécurité en cas d'attaque sur xntpd. L'attaquant ne peut ainsi pas compromettre le système dans son ensemble. *Configurer le démon NTP via DHCP* configure le client NTP pour obtenir la liste des serveurs NTP disponibles sur votre réseau via DHCP.

Les serveurs et autres sources de temps que le client peut interroger sont affichés dans la partie inférieure. Modifiez cette liste selon vos besoins avec *Ajouter*, *Modifier* et *Supprimer*. *Afficher le journal* permet d'afficher les fichiers journaux de votre client.

Cliquez sur *Ajouter* pour ajouter une nouvelle source d'information de temps. Dans la boîte de dialogue suivante, sélectionnez le type de source avec laquelle la synchronisation doit s'effectuer. Vous disposez des options suivantes :

Serveur
: Une autre boîte de dialogue permet de sélectionner un serveur NTP (comme décrit dans Section 44.1.1, « Configuration rapide du client NTP » (p. 704)). Activez *Utiliser pour la Synchronisation initiale* pour déclencher la synchronisation des informations de temps entre le serveur et le client lors du démarrage du système. Un champ d'entrée permet de spécifier des options supplémentaires pour xntpd. Reportez-vous à `/usr/share/doc/packages/xntp-doc` (qui fait partie du paquetage `xntp-doc`) pour obtenir des informations détaillées.

Pair
: Un pair est une machine avec laquelle une relation symétrique est établie : elle agit à la fois comme serveur de temps et comme client. Pour utiliser un pair dans le même réseau au lieu d'un serveur, entrez l'adresse du système. Le reste de la boîte de dialogue est identique à la boîte de dialogue *Serveur*.

Horloge radio
: Pour utiliser une horloge radio dans votre système pour la synchronisation du temps, entrez le type d'horloge, le numéro de l'unité, le nom du périphérique et les autres options dans cette boîte de dialogue. Cliquez sur *Calibration du pilote* pour régler le pilote. Vous trouverez des informations concernant le fonctionnement d'une horloge radio locale dans `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Diffusion sortante
: Les informations de temps et les requêtes peuvent également être transmises par diffusion sur le réseau. Dans cette boîte de dialogue, entrez l'adresse à laquelle ces diffusions doivent être envoyées. N'activez pas la diffusion si vous ne disposez pas d'une source de temps fiable telle qu'une horloge contrôlée par radio.

Diffusion entrante

Si vous souhaitez que votre client reçoive ses informations par diffusion, entrez l'adresse à partir de laquelle les paquets respectifs doivent être acceptés dans ces champs.

44.2 Configuration de xntp dans le réseau

Le moyen le plus simple d'utiliser un serveur de temps dans le réseau consiste à définir les paramètres du serveur. Par exemple, si un serveur de temps nommé `ntp.exemple.com` est accessible à partir du réseau, ajoutez son nom au fichier `/etc/ntp.conf` en ajoutant la ligne `serveur ntp.exemple.com`. Pour ajouter d'autres serveurs de temps, insérez des lignes supplémentaires avec le serveur de mots-clés. Après avoir initialisé xntpd avec la commande `rcxntpd start`, il faut environ une heure pour que l'heure soit stabilisée et que le fichier de dérive de correction de l'horloge de l'ordinateur local soit créé. Avec le fichier de dérive, l'erreur systématique de l'horloge matérielle peut être calculée dès que l'ordinateur est sous tension. La correction est utilisée immédiatement, ce qui se traduit par une stabilité plus grande de l'heure du système.

Il y a deux façons possibles d'utiliser le mécanisme NTP en tant que client. Tout d'abord, le client peut demander l'heure à partir d'un serveur connu à intervalles réguliers. Avec de nombreux clients, cette approche peut provoquer une surcharge sur le serveur. En second lieu, le client peut attendre les diffusions NTP envoyées par les serveurs de temps de diffusion sur le réseau. Cette approche présente les inconvénients suivants : la qualité du serveur est inconnue et un serveur envoyant des informations erronées peut provoquer de graves problèmes.

Si l'heure est obtenue par diffusion, le nom du serveur n'est pas nécessaire. Dans ce cas, entrez la ligne `broadcastclient` dans le fichier de configuration `/etc/ntp.conf`. Pour utiliser un ou plusieurs serveurs de temps exclusivement, entrez leurs noms sur la ligne commençant par `servers`.

44.3 Configuration d'une horloge de référence locale

Le paquetage logiciel xntp contient des pilotes pour la connexion d'horloges de référence locales. La liste des horloges prises en charge est disponible dans le paquetage `xntp-doc` du fichier `/usr/share/doc/packages/xntp-doc/html/refclock.htm`. Chaque pilote est associé à un numéro. Dans xntp, la configuration réelle s'effectue au moyen de pseudo IP. Les horloges sont entrées dans le fichier `/etc/ntp.conf` comme si elles existaient sur le réseau. À cette fin, des adresses IP leur sont assignées sous la forme `127.127.t.u`. Ici, `t` représente le type d'horloge et détermine le pilote utilisé, et `u` représente l'unité, qui détermine l'interface utilisée.

Normalement, les pilotes individuels ont des paramètres spéciaux qui décrivent les détails de la configuration. Le fichier `/usr/share/doc/packages/xntp-doc/html/driverNN.htm` (où `NN` est le numéro du pilote) fournit des informations concernant le type particulier d'horloge. Par exemple, l'horloge « type 8 » (horloge radio sur interface série) nécessite un mode supplémentaire qui spécifie l'horloge plus précisément. Le module récepteur Conrad DCF77, par exemple, a le mode 5. Pour utiliser cette horloge comme référence préférée, spécifiez le mot-clé `prefer`. La ligne `server` complète d'un module récepteur Conrad DCF77 serait la suivante :

```
server 127.127.8.0 mode 5 prefer
```

Les autres horloges suivent le même modèle. À la suite de l'installation du paquetage `xntp-doc`, la documentation de xntp est disponible dans le répertoire `/usr/share/doc/packages/xntp-doc/html`. Le fichier `/usr/share/doc/packages/xntp-doc/html/refclock.htm` fournit des liens vers les pages des pilotes qui en décrivent les paramètres.

45 LDAP - Service d'annuaire

LDAP (Lightweight Directory Access Protocol) est un jeu de protocoles conçu pour l'accès aux annuaires d'informations et leur maintenance. LDAP peut être utilisé à diverses fins, telles que la gestion d'utilisateurs et de groupes, la gestion de configuration système ou la gestion d'adresses. Ce chapitre propose des informations de base sur le fonctionnement d'OpenLDAP et sur la gestion de données LDAP avec YaST. Alors qu'il existe plusieurs implémentations du protocole LDAP, ce chapitre est exclusivement consacré à l'implémentation OpenLDAP.

Au sein d'un environnement réseau, il est crucial de conserver les informations importantes sous une forme structurée et rapidement disponible. Ceci est possible grâce à un service d'annuaire qui, à l'instar des pages jaunes, stocke les informations sous une forme bien structurée et rapidement accessible.

Dans le cas idéal, un serveur central stocke les données dans un annuaire et les distribue à tous les clients par le biais d'un protocole donné. Les données sont structurées de manière à être accessibles par une large palette d'applications. En mettant à disposition un dépôt de données central, cette solution évite que chaque outil d'agenda électronique ou client de messagerie électronique ne gère sa propre base de données. Ceci réduit considérablement les tâches administratives liées aux informations. L'utilisation d'un protocole ouvert et standardisé comme LDAP garantit qu'un maximum d'applications clientes pourra accéder aux données.

Dans ce contexte, l'annuaire est un type de base de données optimisé pour des consultations et des recherches rapides et efficaces :

- Pour rendre de nombreux accès concomitants en lecture possibles, l'accès en écriture est limité à un petit nombre de mises à jour par l'administrateur. Les bases de don-

nées conventionnelles sont optimisées pour accepter le plus gros volume de données possible en un minimum de temps.

- Les accès en écriture étant uniquement possibles de façon restreinte, un service d'annuaire est utilisé pour administrer les informations statiques, généralement inchangées. Les données d'une base de données conventionnelle changent généralement très souvent (données *dynamiques*). Les numéros de téléphone dans l'annuaire d'une entreprise ne changent par exemple pas aussi souvent que les chiffres de la comptabilité.

- Quand des données statiques sont administrées, les mises à jour des données existantes sont très rares. Dans le cadre de données dynamiques, en particulier des données de comptes bancaires ou de comptabilité, la cohérence des données est d'une importance primordiale. Si un montant doit être soustrait d'un endroit pour être ajouté à un autre, les deux opérations doivent intervenir de façon concomitante, au sein d'une *transaction*, pour assurer l'équilibre du stock de données. Les bases de données prennent de telles transactions en charge, contrairement aux annuaires. Les incohérences de données à court terme sont tolérées dans les annuaires.

La conception d'un service d'annuaire comme LDAP n'est pas prévue pour prendre en charge des mécanismes complexes de mise à jour ou de requête. Toutes les applications qui accèdent à ce service doivent pouvoir y accéder rapidement et facilement.

De nombreux services d'annuaire existaient déjà et continuent d'exister sous Unix et ailleurs. Novell NDS, Microsoft ADS, Banyan's Street Talk et le standard OSI X.500 ne sont que quelques exemples. LDAP était initialement prévu comme une version allégée de DAP, le protocole d'accès aux annuaires, qui avait été développé pour les accès X.500. Le standard X.500 réglemente l'organisation hiérarchique des entrées d'annuaire.

LDAP est une version réduite de DAP. Sans perdre la hiérarchie des entrées X.500, profitez des fonctionnalités inter-plates-formes de LDAP et économisez des ressources. L'utilisation de TCP/IP simplifie grandement l'établissement d'interfaces entre une application d'accueil et le service LDAP.

Entre temps, LDAP a évolué et est de plus en plus employé comme solution autonome sans support X.500. LDAP prend en charge les *références* à LDAPv3 (la version du protocole contenue dans le paquetage `openldap2`), ce qui permet la création de bases de données distribuées. L'utilisation de SASL (simple authentication and security layer) est aussi une nouveauté.

LDAP ne se limite pas aux requêtes de données sur les serveurs X.500, comme c'était initialement prévu. Le serveur Open source slapd peut stocker des informations d'objet dans une base de données locale. Il existe également une extension nommée slurpd, responsable de la réplication des serveurs LDAP multiples.

Le paquetage `openldap2` se compose des éléments suivants :

slapd
: Serveur LDAPv3 autonome qui administre les informations d'objet dans une base de données BerkeleyDB.

slurpd
: Programme permettant la réplication des modifications apportées aux données du serveur LDAP local sur d'autres serveurs LDAP installés sur le réseau.

autres outils de maintenance système
: `slapcat`, `slapadd`, `slapindex`

45.1 LDAP vs NIS

L'administrateur système d'Unix utilise traditionnellement le service NIS pour la résolution de noms et la distribution de données dans un réseau. Les données de configuration contenues dans les fichiers de `/etc` et dans les répertoires `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` et `services` sont distribuées par des clients dans l'ensemble du réseau. La maintenance de ces fichiers ne nécessite aucun effort particulier puisqu'il s'agit de simples fichiers texte. La manipulation de grandes quantités de données devient néanmoins de plus en plus difficile en raison de l'absence de structure. NIS est uniquement conçu pour des plates-formes Unix, ce qui rend impossible son utilisation pour un administrateur central des données dans un réseau hétérogène.

À la différence de NIS, le service LDAP ne se limite pas aux réseaux Unix purs. Les serveurs Windows (à partir de 2000) prennent le service d'annuaire LDAP en charge. Novell propose également un service LDAP. Les tâches applicatives mentionnées plus haut sont en outre prises en charge dans les systèmes autres qu'Unix.

Le principe LDAP peut être appliqué à toute structure de données qui doit être administrée de façon centrale. Voici quelques exemples d'applications :

- Utilisation en remplacement du service NIS.
- Routage de courrier (postfix, sendmail).
- Carnets d'adresses pour clients de messagerie, tels que Mozilla, Evolution et Outlook.
- Administration de descriptions de zone pour un serveur de noms BIND9.
- Authentification utilisateur avec Samba dans les réseaux hétérogènes.

Cette liste peut être étendue puisque, contrairement à NIS, LDAP est extensible. La structure hiérarchique clairement définie simplifie l'administration de gros volumes de données en facilitant les recherches.

45.2 Structure d'une arborescence LDAP

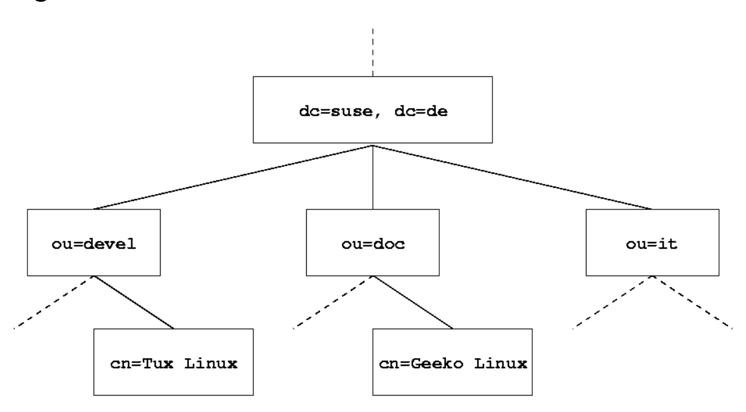
Les annuaires LDAP possèdent une structure arborescente. Toutes les entrées (appelées objets) de l'annuaire ont une position définie au sein de cette hiérarchie. Cette hiérarchie est appelée *DIT (directory information tree)*, c'est-à-dire arborescence d'informations d'annuaire. Le chemin complet menant à une entrée et permettant de l'identifier sans ambiguïté est appelé *nom distinctif* ou DN (distinguished name). Un nœud unique situé le long du chemin vers cette entrée est appelé *nom distinctif relatif* ou RDN (relative distinguished name). Les objets peuvent généralement être affectés à l'un des deux types possibles :

conteneur
: Ces objets peuvent eux-mêmes contenir d'autres objets. Les classes d'objet correspondantes sont `root` (élément racine de l'arborescence, qui n'existe pas réellement), `c` (pays), `ou` (unité organisationnelle) et `dc` (composant de domaine). Ce modèle est comparable aux répertoires (dossiers) d'un système de fichiers.

feuille
: Ces objets se situent en bout de branche et n'ont pas d'objets subordonnés. On peur citer par exemple `person`, `InetOrgPerson` ou `groupofNames`.

Au sommet de la hiérarchie d'annuaire se trouve l'élément racine `root`. Celui-ci accepte les éléments subordonnés de type `c` (pays), `dc` (composant de domaine) ou `o` (organisation). Les relations au sein d'une arborescence d'annuaire LDAP deviennent plus évidentes à la lumière de l'exemple suivant, illustré dans Figure 45.1, « Structure d'un annuaire LDAP » (p. 713).

Figure 45.1 *Structure d'un annuaire LDAP*



L'organigramme complet comprend une arborescence d'informations d'annuaire fictive. Les entrées sont représentées sur trois niveaux. Chaque entrée correspond à une case sur l'image. Le *nom distinctif* complet et valide de l'employé SUSE fictif `Geeko Linux` est `cn=Geeko Linux,ou=doc,dc=suse,dc=de` dans ce cas. Il est formé par adjonction du nom distinctif relatif (RDN) `cn=Geeko Linux` au nom distinctif (DN) de l'entrée précédente `ou=doc,dc=suse,dc=de`.

La détermination globale des types d'objets pouvant être stockés dans la DIT est effectuée suivant un *modèle*. Le type d'un objet est déterminé par la *classe d'objet*. La classe d'objet détermine les attributs devant ou pouvant être affectés à l'objet concerné. Le modèle doit par conséquent contenir des définitions de toutes les classes d'objets et attributs utilisés dans le scénario d'application désiré. Il existe peu de modèles communs (voir RFC 2252 et 2256). Il est néanmoins possible de créer des modèles personnalisés ou d'utiliser plusieurs modèles se complétant mutuellement si l'environnement dans lequel le serveur LDAP doit fonctionner l'exige.

Tableau 45.1, « Classes d'objets et attributs couramment utilisés » (p. 714) offre un petit aperçu des classes d'objets de `core.schema` et `inetorgperson.schema` utilisées dans l'exemple, comprenant les attributs requis et les valeurs d'attributs valides.

Tableau 45.1 Classes d'objets et attributs couramment utilisés

Classe d'objets	Signification	Exemple d'entrée	Attributs obligatoires
dcObject	*domainComponent* (nommez les composants du domaine)	suse	dc
organizationalUnit	*organizationalUnit* (unité organisationnelle)	doc	ou
inetOrgPerson	*inetOrgPerson* (données associées à une personne pour l'intranet ou Internet)	Geeko Linux	sn et cn

Exemple 45.1, « Extrait de schema.core » (p. 714) montre un extrait d'une directive de modèle avec des explications (la numérotation des lignes sert aux explications).

***Exemple 45.1** Extrait de schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: organizational unit this object belongs to'
#3        SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5        DESC 'RFC2256: an organizational unit'
#6        SUP top STRUCTURAL
#7        MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
    $ x121Address $ registeredAddress $ destinationIndicator
    $ preferredDeliveryMethod $ telexNumber
    $ teletexTerminalIdentifier $ telephoneNumber
    $ internationaliSDNNumber $ facsimileTelephoneNumber
    $ street $ postOfficeBox $ postalCode $ postalAddress
    $ physicalDeliveryOfficeName
    $ st $ l $ description) )
...
```

Le type d'attribut `organizationalUnitName` et la classe d'objet correspondante `organizationalUnit` servent ici d'exemple. La ligne 1 indique le nom de l'attribut, son OID unique (*identificateur d'objet*) (numérique) et l'abréviation de l'attribut.

La ligne 2 donne une brève description de l'attribut avec DESC. La requête RFC correspondante, sur laquelle la définition est basée, est également mentionnée ici. Dans la ligne 3, SUP indique un type d'attribut générique auquel appartient cet attribut.

La définition de la classe d'objet organizationalUnit commence à la ligne 4, comme pour la définition de l'attribut, avec un OID et le nom de la classe d'objet. La ligne 5 contient une brève description de la classe d'objet. L'entrée SUP top dans la ligne 6 indique que cette classe d'objet n'est pas subordonnée à une autre classe d'objet. La ligne 7, qui commence par MUST, répertorie tous les types d'attributs qui *doivent* être utilisés en association avec un objet de type organizationalUnit. La ligne 8, introduite par MAY, répertorie tous les types d'attributs qui sont autorisés en association avec cette classe d'objet.

Une très bonne introduction à l'utilisation de modèles est disponible dans la documentation sur OpenLDAP. Si elle est installée, vous la trouverez dans /usr/share/doc/packages/openldap2/admin-guide/index.html.

45.3 Configuration de serveur avec slapd.conf

Votre système comporte un fichier de configuration complet pour le serveur LDAP dans /etc/openldap/slapd.conf. Les entrées individuelles sont succinctement décrites ici et les ajustements nécessaires sont expliqués. Les entrées introduites par le signe dièse (#) sont inactives. Supprimez ce caractère de commentaire pour les activer.

45.3.1 Directives globales dans slapd.conf

Exemple 45.2 *slapd.conf : directive include pour les modèles*

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

Cette première directive dans slapd.conf, illustrée dans Exemple 45.2, « slapd.conf : directive include pour les modèles » (p. 715), spécifie le modèle selon lequel l'annuaire LDAP est organisé. L'entée core.schema est obligatoire. Les modèles supplémen-

taires requis sont ajoutés à cette directive. Des informations sont disponibles dans la documentation OpenLDAP incluse.

Exemple 45.3 *slapd.conf : pidfile et argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Ces deux fichiers contiennent le PID (ID de processus) et certains des arguments avec lesquels le processus `slapd` est démarré. Aucune modification n'est requise ici.

Exemple 45.4 *slapd.conf : contrôle d'accès*

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
              by users read
              by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

Exemple 45.4, « slapd.conf : contrôle d'accès » (p. 716) est l'extrait de `slapd.conf` qui réglemente les autorisations d'accès pour l'annuaire LDAP sur le serveur. Les paramètres définis ici dans la section globale de `slapd.conf` sont valides tant qu'aucune règle d'accès personnalisée n'est définie dans la section spécifique aux bases de données. Ces dernières remplacent en effet les déclarations générales. Comme indiqué ici, tous les utilisateurs ont accès à l'annuaire en lecture, mais seul l'administrateur (`rootdn`) dispose de droits d'écriture. La réglementation du contrôle d'accès dans LDAP est un processus hautement complexe. Les astuces suivantes peuvent être utiles :

- Chaque règle d'accès possède la structure suivante :

  ```
  access to <what> by <who> <access>
  ```

- *`what`* désigne l'emplacement pour l'objet ou l'attribut auquel l'accès est donné. Des branches individuelles de l'annuaire peuvent être protégées explicitement à l'aide de règles séparées. Il est également possible de traiter des portions de l'arborescence d'annuaire avec une règle en utilisant des expressions régulières. `slapd` évalue toutes les règles dans l'ordre où elles sont répertoriées dans le fichier de

configuration. Les règles plus générales doivent figurer après les règles plus spécifiques : la première règle `slapd` est considérée comme valide et toutes les entrées suivantes sont ignorées.

- *`who`* détermine qui doit avoir accès aux zones définies par *`what`*. Des expressions régulières peuvent être employées. `slapd` annule à nouveau l'évaluation de `who` après la première correspondance. Les règles plus spécifiques doivent donc être spécifiées avant les règles plus générales. Les entrées illustrées dans Tableau 45.2, « Groupes d'utilisateurs et autorisations d'accès » (p. 717) sont possibles.

Tableau 45.2 *Groupes d'utilisateurs et autorisations d'accès*

Étiquette	Portée
`*`	Tous les utilisateurs sans exception.
`anonymous`	Utilisateurs non authentifiés (« anonymes »).
`users`	Utilisateurs authentifiés.
`self`	Utilisateurs connectés à l'objet cible.
`dn.regex=<regex>`	Tous les utilisateurs correspondant à l'expression régulière.

- *`access`* spécifie le type d'accès. Utilisez les options répertoriées dans Tableau 45.3, « Types d'accès » (p. 717).

Tableau 45.3 *Types d'accès*

Étiquette	Portée de l'accès
`none`	Aucun accès.
`auth`	Pour contacter le serveur.
`compare`	Accès aux objets pour comparaison.

Étiquette	Portée de l'accès
search	Pour l'emploi de filtres de recherche.
read	Accès en lecture.
write	Accès en écriture.

slapd compare les droits d'accès requis par le client à ceux accordés dans slapd.conf. Le client se voit accorder l'accès si les autorisations sont supérieures ou égales à celles demandées. Si le client demande des droits supérieurs à ceux qui sont déclarés dans les règles, l'accès lui est refusé.

Exemple 45.5, « slapd.conf : exemple de contrôle d'accès » (p. 718) illustre un exemple de contrôle d'accès simplifié pouvant être développé arbitrairement à l'aide d'expressions régulières.

***Exemple 45.5** slapd.conf : exemple de contrôle d'accès*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

Cette règle déclare que seul l'administrateur correspondant possède des droits d'accès à une entrée ou individuelle. Les utilisateurs authentifiés disposent d'un accès en lecture, tandis que tous les autres n'ont aucun accès.

ASTUCE: Définition de règles d'accès

En l'absence de règle access to ou de directive by correspondante, l'accès est refusé. Seuls les droits d'accès explicitement déclarés sont accordés. Si aucune règle n'est déclarée, le principe par défaut consiste à accorder des droits d'accès en écriture à l'administrateur et un accès en lecture à tous les autres utilisateurs.

Vous trouverez des informations détaillées et un exemple de configuration de droits d'accès LDAP dans la documentation en ligne du paquetage openldap2 installé.

Hormis le fichier central de configuration du serveur (slapd.conf), les autorisations d'accès peuvent également être administrées par le biais des informations de contrôle

d'accès (ACI). ACI permet le stockage d'informations d'accès pour des objets individuels au sein de l'arborescence LDAP. Ce type de contrôle d'accès reste peu fréquent et est considéré comme expérimental par les développeurs. Consultez `http://www.openldap.org/faq/data/cache/758.html` pour plus d'informations.

45.3.2 Directives spécifiques aux bases de données dans slapd.conf

Exemple 45.6 *slapd.conf : directives spécifiques aux bases de données*

```
database bdb
checkpoint      1024    5
cachesize       10000
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

Le type de base de données, Berkeley dans ce cas, est déterminé dans les premières lignes de cette section (voir Exemple 45.6, « slapd.conf : directives spécifiques aux bases de données » (p. 719)). `checkpoint` détermine la quantité de données (en ko) conservée dans le journal des transactions avant d'être transférée dans la base de données et le temps (en minutes) séparant deux actions d'écriture. `cachesize` définit le nombre d'objets conservés dans le cache de la base de données. `suffix` détermine la portion de l'arborescence LDAP dont ce serveur doit être responsable. `rootdn` détermine ensuite qui bénéficie de droits d'administrateur sur ce serveur. L'utilisateur déclaré ici n'a pas besoin d'avoir une entrée LDAP ou d'exister en tant qu'utilisateur normal. Le mot de passe d'administrateur est défini avec `rootpw`. Au lieu d'utiliser `secret` ici, il est possible de saisir le hachage du mot de passe d'administrateur créé par `slappasswd`. La directive `directory` indique le répertoire (dans le système de fichiers) dans lequel les annuaires de bases de données sont stockés sur le serveur. La dernière directive, `index objectClass eq`, entraîne la maintenance d'un index de toutes les classes d'objet. Les attributs les plus fréquemment recherchés par les utilisateurs peuvent être ajoutés ici d'après l'expérience. Les règles `Access` personnalisées définies ici pour la base de données sont utilisées en lieu et place des règles `Access` générales.

45.3.3 Démarrage et arrêt des serveurs

Quand le serveur LDAP est entièrement configuré et que toutes les entrées souhaitées ont été effectuées conformément au modèle décrit dans Section 45.4, « Gestion de données dans l'annuaire LDAP » (p. 720), démarrez le serveur LDAP en tant que `root` en tapant `rcldap start` . Pour arrêter manuellement le serveur, saisissez la commande `rcldap stop` . Pour interroger l'état du serveur LDAP en cours d'exécution, tapez `rcldap status` .

L'éditeur de niveaux d'exécution de YaST, décrit dans Section 28.2.3, « Configuration des services système (niveau d'exécution) avec YaST » (p. 465), peut être utilisé pour configurer le démarrage et l'arrêt automatique du serveur à l'amorçage et à l'arrêt du système. Il est également possible de créer des liens correspondants aux scripts de démarrage et d'arrêt avec la commande `insserv` depuis une invite de commande, conformément à ce qui est décrit dans Section 28.2.2, « Scripts d'initialisation » (p. 460).

45.4 Gestion de données dans l'annuaire LDAP

OpenLDAP propose une série d'outils pour l'administration de données dans l'annuaire LDAP. Les quatre principaux outils permettant d'ajouter, de supprimer, de rechercher ou de modifier des données sont brièvement présentés ci-dessous.

45.4.1 Insertion de données dans un annuaire LDAP

Lorsque la configuration de votre serveur LDAP dans `/etc/openldap/lsapd.conf` est correcte et prête à l'emploi (c'est-à-dire qu'elle comporte des entrées appropriées pour `suffix`, `directory`, `rootdn`, `rootpw` et `index`), procédez à la saisie des enregistrements. OpenLDAP dispose de la commande `ldapadd` à cet effet. Si possible, ajoutez les objets à la base de données par lots pour des raisons pratiques. LDAP est en mesure de traiter le format LDIF (LDAP data interchange format) pour ceci. Un fichier LDIF est un simple fichier texte pouvant contenir un nombre variable de couples attribut-valeur. Reportez-vous aux fichiers de modèles déclarés dans `slapd.conf` pour connaître les classes et attributs d'objets disponibles. Le fichier LDIF pour

la création d'une ébauche de structure pour l'exemple dans Figure 45.1, « Structure d'un annuaire LDAP » (p. 713) ressemblerait à celui dans Exemple 45.7, « Exemple pour un fichier LDIF » (p. 721).

Exemple 45.7 *Exemple pour un fichier LDIF*

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

IMPORTANT: Codage des fichiers LDIF

LDAP fonctionne avec UTF-8 (Unicode). Les trémas doivent être codés correctement. Utilisez un éditeur qui prend UTF-8 en charge, tel que Kate ou une version récente d'Emacs. Sinon, évitez les trémas et autres caractères spéciaux ou utilisez `recode` pour recoder la saisie en UTF-8.

Enregistrez le fichier avec l'extension `.ldif` puis envoyez-le au serveur à l'aide de la commande suivante :

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

`-x` désactive l'authentification avec SASL dans ce cas. `-D` déclare l'utilisateur qui appelle l'opération. Le DN valide de l'administrateur est saisi ici exactement comme il a été configuré dans `slapd.conf`. Dans cet exemple, c'est-à-dire `cn=admin,dc=suse,dc=de`. `-W` évite la saisie du mot de passe sur la ligne de commandes (en texte clair) et active une invite de mot de passe séparée. Ce mot de passe a été défini précédemment dans `slapd.conf` avec `rootpw`. `-f` transmet le

nom de fichier. Des détails sur le fonctionnement de `ldapadd` peuvent être consultés dans Exemple 45.8, « ldapadd avec example.ldif » (p. 722).

Exemple 45.8 *ldapadd avec example.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Les données utilisateur individuelles peuvent être préparées dans des fichiers LDIF séparés. Exemple 45.9, « Données LDIF pour Tux » (p. 722) ajoute `Tux` au nouvel annuaire LDAP.

Exemple 45.9 *Données LDIF pour Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Un fichier LDIF peut contenir un nombre quelconque d'objets. Il est possible de transmettre au serveur des branches entières d'annuaire en une fois ou uniquement des parties comme le montre l'exemple des objets individuels. Si des données doivent être modifiées de façon relativement fréquente, une subdivision fine des objets individuels est recommandée.

45.4.2 Modification de données dans l'annuaire LDAP

L'outil `ldapmodify` est fourni pour modifier le stock de données. La meilleure façon pour ce faire consiste à modifier le fichier LDIF correspondant avant de transmettre ce fichier modifié au serveur LDAP. Pour modifier le numéro de téléphone du collègue Tux de `+49 1234 567-8` en `+49 1234 567-10`, modifiez le fichier LDIF comme dans Exemple 45.10, « Fichier LDIF tux.ldif modifié » (p. 723).

Exemple 45.10 *Fichier LDIF tux.ldif modifié*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importez le fichier modifié dans l'annuaire LDAP à l'aide de la commande suivante :

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Vous pouvez aussi transmettre directement les attributs à modifier à `ldapmodify`. La procédure correspondante est décrite ci-dessous :

1. Démarrez `ldapmodify` et saisissez votre mot de passe :

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W
   Enter LDAP password:
   ```

2. Saisissez les modifications en respectant scrupuleusement la syntaxe dans l'ordre indiqué ci-dessous :

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Vous trouverez des informations détaillées sur `ldapmodify` et sa syntaxe dans la page d'aide de ldapmodify(1).

45.4.3 Recherche ou lecture de données dans un annuaire LDAP

Avec `ldapsearch` OpenLDAP fournit un outil de ligne de commande pour la recherche de données au sein d'un annuaire LDAP et pour la lecture de données depuis ce dernier. Une requête simple emploierait la syntaxe suivante :

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

L'option `-b` détermine la base de recherche, c'est-à-dire la section de l'arborescence au sein de laquelle la recherche doit être menée. Dans ce cas, il s'agit de `dc=suse,dc=de`. Pour procéder à une recherche plus fine dans des sous-sections spécifiques de l'annuaire

LDAP (par exemple, uniquement dans le département `devel`), transmettez cette section à `ldapsearch` avec `-b`. `-x` demande l'activation de l'authentification simple. `(objectClass=*)` indique que tous les objets contenus dans l'annuaire doivent être lus. Cette option de commande peut être utilisée après création d'une nouvelle arborescence d'annuaire pour vérifier que toutes les entrées ont été enregistrées correctement et que le serveur répond comme voulu. Vous trouverez de plus amples informations sur l'utilisation de `ldapsearch` dans la page d'aide correspondante (ldapsearch(1)).

45.4.4 Suppression de données d'un annuaire LDAP

Supprimez les entrées superflues avec `ldapdelete`. La syntaxe est similaire à celle des commandes décrites plus haut. Par exemple, pour supprimer l'entrée complète de `Tux Linux`, utilisez la commande suivante :

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

45.5 Client LDAP de YaST

YaST comprend un module pour la configuration d'une gestion utilisateur basée sur LDAP. Si vous n'avez pas activé cette fonction durant l'installation, démarrez le module en cliquant sur *Services réseau* → *Client LDAP*. YaST active automatiquement des modifications liées à PAM et NSS requises par LDAP (voir plus bas) et installe les fichiers nécessaires.

45.5.1 Procédure standard

Les connaissances de fond sur les processus fonctionnant en arrière-plan d'une machine cliente vous aident à comprendre le fonctionnement du module client LDAP de YaST. Si LDAP est activé pour l'authentification réseau ou si le module YaST est appelé, les paquetages `pam_ldap` et `nss_ldap` sont installés et les deux fichiers de configuration correspondants sont adaptés. `pam_ldap` est le module PAM responsable de la négociation entre les processus de login et l'annuaire LDAP comme source de données d'authentification. Le module dédié `pam_ldap.so` est installé et la configuration PAM est adaptée (voir Exemple 45.11, « pam_unix2.conf adapté à LDAP » (p. 725)).

Exemple 45.11 *pam_unix2.conf adapté à LDAP*

```
auth:        use_ldap
account:     use_ldap
password:    use_ldap
session:     none
```

Lorsque vous configurez manuellement des services supplémentaires pour LDAP, incluez le module LDAP PAM dans le fichier de configuration PAM correspondant au service dans `/etc/pam.d`. Des fichiers de configuration déjà adaptés aux services individuels sont disponibles dans `/usr/share/doc/packages/pam_ldap/pam.d/`. Copiez les fichiers appropriés dans `/etc/pam.d`.

La résolution de nom `glibc` par l'intermédiaire du mécanisme `nsswitch` est adaptée à l'utilisation de LDAP avec `nss_ldap`. Un nouveau fichier `nsswitch.conf` adapté est créé dans `/etc/` avec l'installation de ce paquetage. Vous trouverez de plus amples informations sur le fonctionnement de `nsswitch.conf` dans Section 38.5.1, « Fichiers de configuration » (p. 638). Les lignes suivantes doivent figurer dans `nsswitch.conf` pour permettre l'administration et l'authentification des utilisateurs avec LDAP. Voir Exemple 45.12, « Adaptations dans nsswitch.conf » (p. 725).

Exemple 45.12 *Adaptations dans nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Ces lignes ordonnent à la bibliothèque resolver de `glibc` d'évaluer d'abord les fichiers correspondants dans `/etc`, puis d'accéder au serveur LDAP comme sources d'authentification et de données d'utilisateurs. Testez ce mécanisme, par exemple en lisant le contenu de la base de données des utilisateurs avec la commande `getent passwd` . L'ensemble de résultats renvoyés doit contenir un relevé des utilisateurs locaux de votre système ainsi que tous les utilisateurs stockés sur le serveur LDAP.

Pour empêcher les utilisateurs ordinaires gérés par LDAP de se connecter au serveur avec `ssh` ou `login`, les fichiers `/etc/passwd` et `/etc/group` doivent chacun inclure une ligne supplémentaire. Il s'agit des lignes `+::::::/sbin/nologin` dans `/etc/passwd` et `+:::` dans `/etc/group`.

45.5.2 Configuration du client LDAP

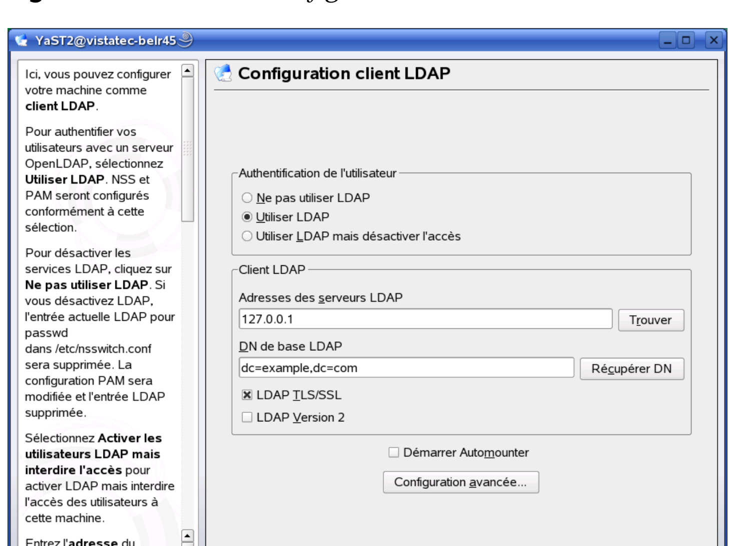
Après que les ajustements initiaux de `nss_ldap`, `pam_ldap`, `/etc/passwd` et `/etc/group` ont été effectués par YaST, vous pouvez connecter simplement votre client au serveur et laisser YaST s'occuper de la gestion des utilisateurs via LDAP. La configuration de base est décrite dans la section intitulée « Configuration de base » (p. 726).

Utilisez le client LDAP de YaST pour configurer plus avant les modules de configuration des groupes et des utilisateurs de YaST. Ceci comprend la modification des paramètres par défaut pour les nouveaux utilisateurs et groupes, ainsi que celle du nombre et de la nature des attributs affectés à un utilisateur ou groupe. La gestion d'utilisateurs LDAP permet d'affecter des attributs nettement plus nombreux et plus diversifiés aux utilisateurs et aux groupes que les solutions classiques de gestion des utilisateurs ou des groupes. Ceci est décrit dans la section intitulée « Configuration des modules d'administration de groupes et d'utilisateurs de YaST » (p. 729).

Configuration de base

La boîte de dialogue de configuration de base du client LDAP (Figure 45.2, « YaST : Configuration du client LDAP » (p. 727)) s'ouvre durant l'installation si vous optez pour la gestion des utilisateurs LDAP ou si vous sélectionnez *Services réseau* → *Client LDAP* dans le centre de contrôle YaST de votre système.

Figure 45.2 YaST : Configuration du client LDAP



Pour authentifier les utilisateurs de votre machine face à un serveur OpenLDAP et permettre la gestion des utilisateurs via OpenLDAP, procédez comme suit :

1. Cliquez sur *Utiliser LDAP* pour permettre l'utilisation de LDAP. Sélectionnez plutôt *Utiliser LDAP mais désactiver l'accès* si vous voulez utiliser LDAP pour l'authentification, mais si vous ne souhaitez pas que d'autres utilisateurs se loguent à ce client.

2. Saisissez l'adresse IP du serveur LDAP à utiliser.

3. Saisissez le *DN de base LDAP* pour sélectionner la base de recherche sur le serveur LDAP.

4. Si une communication sécurisée de type TLS ou SSL est requise avec le serveur, sélectionnez *LDAP TLS/SSL*.

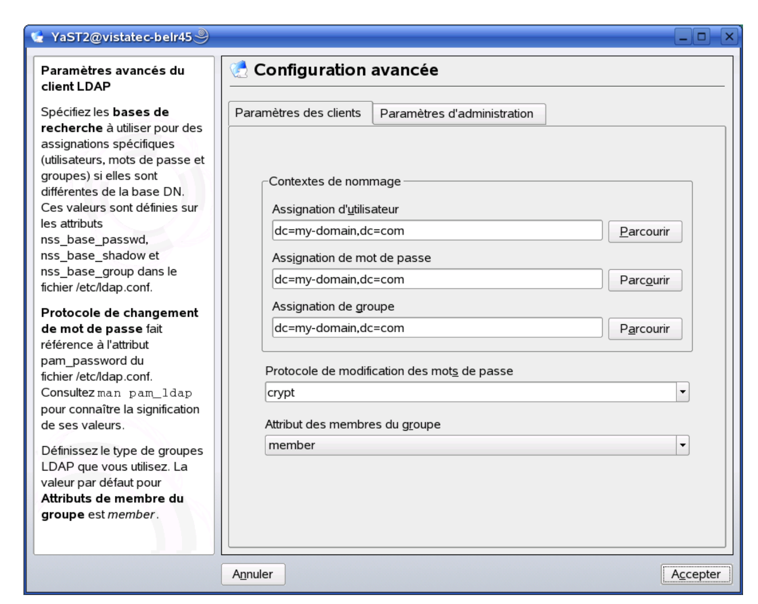
5. Si le serveur LDAP utilise encore LDAPv2, autorisez explicitement l'utilisation de cette version du protocole en sélectionnant *LDAP Version 2*.

6. Sélectionnez *Démarrer Automounter* pour monter les répertoires distants sur votre client, comme un répertoire `/home` géré à distance.

7 Cliquez sur *Terminer* pour appliquer vos réglages.



Figure 45.3 *YaST : Configuration avancée*



Pour modifier des données sur le serveur en tant qu'administrateur, cliquez sur *Configuration avancée*. La boîte de dialogue suivante se subdivise en deux onglets. Voir Figure 45.3, « YaST : Configuration avancée » (p. 728).

1 Sous l'onglet *Paramètres des clients*, ajustez les paramètres suivants en fonction de vos besoins :

a Si la base de recherche pour les utilisateurs, mots de passe et groupes diffère de la base de recherche globale spécifiée par *DN de base LDAP*, saisissez les différents contextes de nommage dans *Assignation d'utilisateur*, *Assignation de mot de passe* et *Assignation de groupe*.

b Spécifiez le protocole de changement du mot de passe. La méthode standard à utiliser pour modifier un mot de passe est `crypt`, c'est-à-dire que le hachage de mot de passe généré par `crypt` est utilisé. Pour plus de détails sur cette option ou d'autres, consultez la page d'aide de `pam_ldap`.

c Spécifiez le groupe LDAP à utiliser avec *Attribut des membres du groupe*. La valeur par défaut de ce champ est `member`.

2 Sous *Paramètres d'administration*, effectuez les réglages suivants :

a Définissez la base de stockage de vos données de gestion utilisateur via *Configuration du DN de base*.

b Entrez la valeur appropriée pour *DN de l'administrateur*. Ce DN doit être identique à la valeur `rootdn` spécifiée dans `/etc/openldap/slapd.conf` pour permettre à cet utilisateur en particulier de manier les données stockées sur le serveur LDAP.

c Cochez *Créer les objets de configuration par défaut* pour créer les objets de configuration de base sur le serveur afin de permettre la gestion des utilisateurs via LDAP.

d Si votre machine cliente doit jouer le rôle de serveur de fichiers pour les répertoires personnels de votre réseau, cochez l'option *Répertoires personnels de cette machine*.

e Cliquez sur *Accepter* pour quitter la *configuration avancée* puis sur *Terminer* pour appliquer vos réglages.

Utilisez *Configurer les paramètres de gestion des utilisateurs* pour modifier les entrées du serveur LDAP. L'accès aux modules de configuration sur le serveur est alors accordé d'après les ACL et ACI stockés sur le serveur. Suivez les procédures décrites dans la section intitulée « Configuration des modules d'administration de groupes et d'utilisateurs de YaST » (p. 729).

Configuration des modules d'administration de groupes et d'utilisateurs de YaST

Utilisez le client LDAP de YaST pour ajuster les modules d'administration de groupes et d'utilisateurs de YaST et pour les étendre si nécessaire. Définissez des modèles avec des valeurs par défaut pour les attributs individuels afin de simplifier l'enregistrement des données. Les valeurs prédéfinies ici sont stockées comme objets LDAP dans l'annuaire LDAP. L'enregistrement de données utilisateur s'effectue toujours avec les

modules normaux de YaST pour la gestion des utilisateurs et des groupes. Les données enregistrées sont stockées sur le serveur comme objets LDAP.

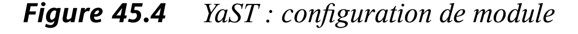
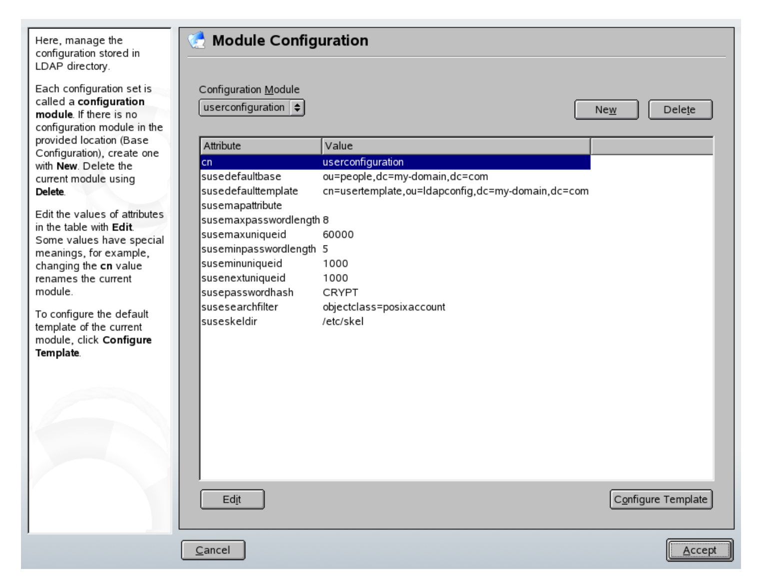


Figure 45.4 *YaST : configuration de module*



La boîte de dialogue de configuration de module (Figure 45.4, « YaST : configuration de module » (p. 730)) permet la création de nouveaux modules, la sélection et la modification des modules de configuration existants, ainsi que la conception et la modification de modèles pour ce type de modules.

Pour créer un module de configuration, procédez comme suit :

1. Cliquez sur *Nouveau* et sélectionnez le type de module à créer. Sélectionnez `suseuserconfiguration` pour un module de configuration d'utilisateurs et `susegroupconfiguration` pour un module de configuration de groupes.

2. Choisissez un nom pour le nouveau modèle.

   La vue du contenu affiche alors un tableau répertoriant tous les attributs autorisés dans ce module avec les valeurs qui leur sont affectées. Hormis les attributs définis, la liste contient également tous les autres attributs autorisés par le modèle en cours mais inutilisés pour le moment.

3 Acceptez les valeurs prédéfinies ou ajustez les valeurs par défaut à utiliser pour la configuration de groupes et d'utilisateurs, en sélectionnant les attributs respectifs, en cliquant sur *Modifier* et en saisissant la nouvelle valeur. Renommez un module simplement en changeant l'attribut `cn` du module. Un clic sur *Effacer* supprime le module sélectionné.

4 Lorsque vous cliquez sur *OK*, le nouveau module est ajouté au menu de sélection.

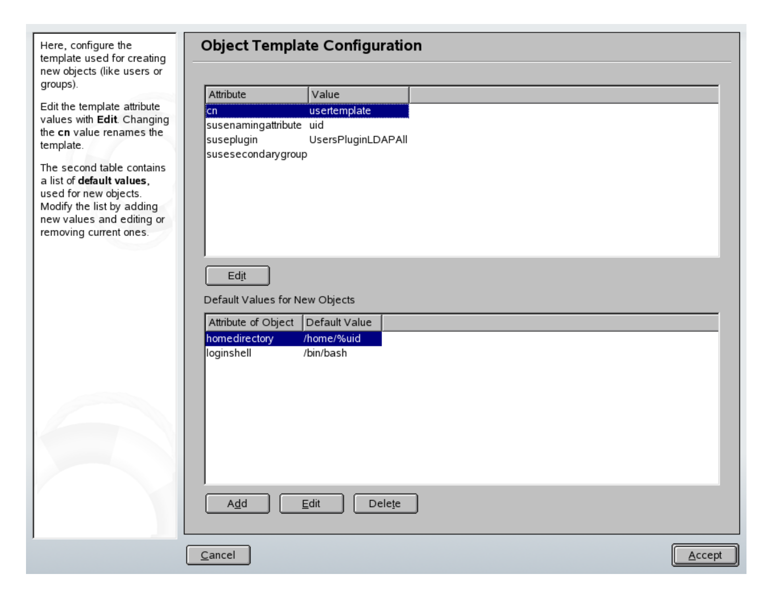
Les modules d'administration de groupes et d'utilisateurs de YaST intègrent des modèles avec des valeurs standard sensibles. Pour modifier un modèle associé à un module de configuration, procédez comme suit :

1 Dans la boîte de dialogue *Configuration du module*, cliquez sur *Configurer le modèle*.

2 Déterminez les valeurs des attributs généraux affectés à ce modèle en fonction de vos besoins ou laissez-en certains vierges. Les attributs vides sont supprimés du serveur LDAP.

3 Modifiez, supprimez ou ajoutez des valeurs par défaut pour les nouveaux objets (objets de configuration d'utilisateur ou de groupe dans l'arborescence LDAP).

Figure 45.5 *YaST : configuration d'un modèle d'objet*



Connectez le modèle à son module en réglant la valeur de l'attribut `susedefaulttemplate` du module sur le DN du modèle adapté.

ASTUCE

Les valeurs par défaut d'un attribut peuvent être créées à partir d'autres attributs en utilisant un style de variable au lieu d'une valeur absolue. Par exemple, lors de la création d'un nouvel utilisateur, `cn=%sn %givenName` est créé automatiquement à partir des valeurs d'attributs pour `sn` et `givenName`.

Quand tous les modules et modèles sont configurés correctement et fonctionnels, de nouveaux groupes et utilisateurs peuvent être enregistrés comme de coutume avec YaST.

45.6 Configuration d'utilisateurs et de groupes LDAP dans YaST

L'enregistrement de données d'utilisateur et de groupe ne diffère que légèrement de la procédure sans LDAP. Les instructions succinctes ci-après ont trait à l'administration des utilisateurs. La procédure d'administration des groupes est analogue.

1. Pour accéder à l'administration d'utilisateurs dans YaST, utilisez *Security & Users (Sécurité et utilisateurs)* → *User Administration (Administration des utilisateurs)*.

2. Utilisez *Définir le filtre* pour limiter l'affichage aux utilisateurs LDAP et saisissez le mot de passe pour le DN root.

3. Cliquez sur *Ajouter* et saisissez la configuration d'un nouvel utilisateur. Une boîte de dialogue s'ouvre avec quatre onglets.

   a. Spécifiez un nom d'utilisateur, un login et un mot de passe sous l'onglet *Données de l'utilisateur*.

   b. Consultez l'onglet *Détails* pour définir l'appartenance à un groupe, le shell de login et le répertoire privé du nouvel utilisateur. Si nécessaire, modifiez les valeurs par défaut afin de mieux les adapter à vos besoins. Les valeurs par défaut, ainsi que les paramètres de mot de passe, peuvent être définis à

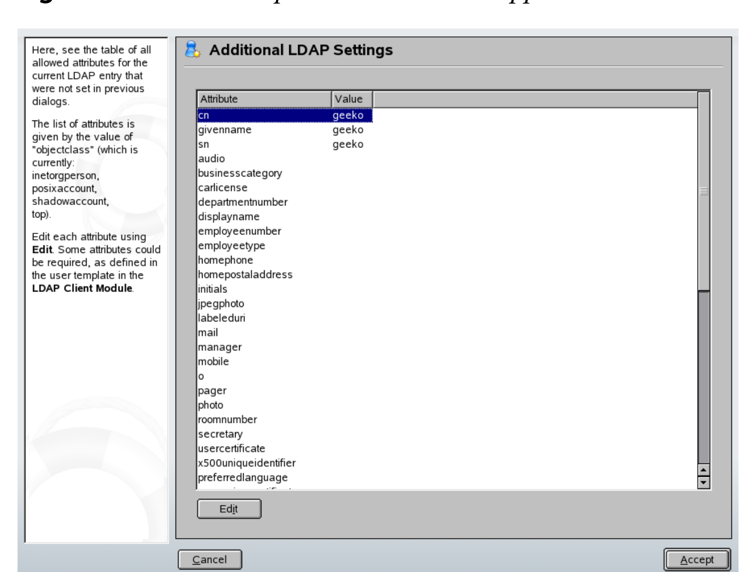
l'aide de la procédure décrite dans la section intitulée « Configuration des modules d'administration de groupes et d'utilisateurs de YaST » (p. 729).

c Modifiez ou acceptez les *Paramètres du mot de passe* par défaut.

d Ouvrez l'onglet *Plug-ins*, sélectionnez le plug-in LDAP et cliquez sur *Lancer* pour configurer des attributs LDAP supplémentaires assignés au nouvel utilisateur (voir Figure 45.6, « YaST : paramètres LDAP supplémentaires » (p. 733)).

4 Cliquez sur *Accepter* pour appliquer vos paramètres et quitter la configuration des utilisateurs.

Figure 45.6 *YaST : paramètres LDAP supplémentaires*



Le formulaire de saisie initial pour l'administration des utilisateurs propose des *options LDAP*. Ceci permet d'appliquer des filtres de recherche LDAP aux utilisateurs disponibles ou de se rendre dans le module de configuration des utilisateurs ou groupes LDAP en sélectionnant *Configuration utilisateur et groupe LDAP*.

45.7 Pour plus d'informations

Des sujets plus complexes, comme la configuration SASL ou l'établissement d'un serveur de réplication LDAP répartissant la charge de travail sur plusieurs esclaves, n'ont volontairement pas été traités dans ce chapitre. Vous trouverez des informations détaillées sur ces deux thèmes dans le *OpenLDAP 2.2 Administrator's Guide (Guide de l'administrateur OpenLDAP 2.2)* (références ci-après).

Le site Web du projet OpenLDAP propose également une documentation exhaustive pour les utilisateurs novices et expérimentés de LDAP.

OpenLDAP Faq-O-Matic
: Base très complète de questions-réponses à propos de l'installation, de la configuration et de l'utilisation de OpenLDAP. Rendez-vous à l'adresse `http://www.openldap.org/faq/data/cache/1.html`.

Quick Start Guide (Guide de démarrage rapide)
: Instructions pas à pas pour l'installation de votre premier serveur LDAP. Rendez-vous à l'adresse `http://www.openldap.org/doc/admin22/quickstart.html` ou dans `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html` sur un système installé.

OpenLDAP 2.2 Administrator's Guide (Guide de l'administrateur OpenLDAP 2.2)
: Présentation détaillée de tous les aspects importants de la configuration LDAP, y compris le contrôle d'accès et le cryptage. Rendez-vous à l'adresse `http://www.openldap.org/doc/admin22/` ou dans `/usr/share/doc/packages/openldap2/admin-guide/index.html` sur un système installé.

Understanding LDAP (Présentation de LDAP)
: Présentation globale détaillée des principes de base de LDAP : `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`.

Ouvrages imprimés traitant de LDAP :

- *LDAP System Administration (Administration système de LDAP)* de Gerald Carter (ISBN 1-56592-491-6).

- *Understanding and Deploying LDAP Directory Services (Présentation et déploiement des services de répertoire LDAP)* de Howes, Smith et Good (ISBN 0-672-32316-8).

Dernière source d'informations sur le sujet LDAP : les RFC (requêtes de commentaires) correspondantes, 2251 à 2256.

46 Le serveur Web Apache

Avec une part de marché supérieure à 60 %, Apache est le serveur Web le plus utilisé au monde selon http://www.netcraft.com. Pour les applications Web, Apache est souvent utilisé sur Linux, avec la base de données MySQL, et les langages de programmation PHP et Perl. Cette combinaison est souvent nommée LAMP.

Ce chapitre introduit le logiciel serveur Web et d'applications Apache dans sa version 2.x. L'installation et la configuration d'Apache sont expliquées ici, ainsi que l'utilisation de certains des modules disponibles.

46.1 Préface et terminologie

Cette section fournit les définitions des termes fréquemment utilisés, qu'ils soient liés au Web ou spécifiques à Apache.

IMPORTANT: Terminologie

Dans ce document, le terme *Apache* se réfère à Apache dans sa version 2.x. Pour obtenir la documentation d'Apache 1.x, consultez le site Web d'Apache.

46.1.1 Serveur Web

Un serveur Web fournit les pages Web demandées par un client. Le client peut être un navigateur Web, tel que Konqueror, ou tout autre périphérique pouvant se connecter

sur le Web. Ces pages peuvent être stockées ensemble sur disque (pages statiques) ou générées en réponse à une demande (pages dynamiques) d'une entité externe, telle qu'une base de données ou un service Web.

46.1.2 HTTP

La communication entre le client et le serveur Web s'effectue en utilisant le protocole HTTP (hypertext transfer protocol). La version actuelle, HTTP 1.1, est documentée dans RFC 2068 et dans la mise à jour RFC 2616. Ces RFC sont disponibles à l'adresse `http://www.w3.org`.

46.1.3 URL

URL signifie universal resource locator (localisateur de ressources universel). Les clients utilisent des URL, telles que `http://www.example.com/index.html`, pour demander des pages du serveur. Une adresse URL est constituée de :

Protocole

Protocoles fréquemment utilisés :

http://

Le protocole HTTP

https://

Version sécurisée, codée de HTTP

ftp://

Protocole de transfert de fichiers pour le téléchargement des fichiers

Domaine

Dans notre exemple, le domaine est `www.example.com`. Le domaine est le nom qui correspond à une adresse IP. Ainsi, `www.example.com` correspond de façon unique à une adresse IP telle que 123.456.789.1. À son tour, le nombre identifie de façon unique l'ordinateur qui exécute un serveur Web. L'assignation d'un nom de domaine à une adresse IP est souvent nommée *résolution de nom*. Le domaine peut être subdivisé en plusieurs parties, ici : `www`, `exemple` et `com`. La dernière partie

du nom de domaine est le domaine de niveau supérieur (TLD). Dans notre exemple, `com` est le TLD. TLD représente le niveau supérieur du processus de résolution de nom. Les TLD peuvent être génériques (les gTLD, tels que `com`, `org` et `net`) ou dépendre du pays (les ccTLD, tels que `fr` pour France). Toutes les parties d'un domaine prises ensemble sont désignées en tant que nom de domaine pleinement qualifié (FQDN).

Ressource

Dans notre exemple, la ressource est `index.html`. Cette partie spécifie le chemin d'accès complet à la ressource. La ressource peut être un fichier, comme dans cet exemple. Elle peut également être un script CGI, une page JavaServer, ou une autre ressource.

Le mécanisme Internet responsable, tel que le système de nom de domaine (DNS), adresse la requête au domaine `www.example.com` à un ou plusieurs ordinateurs contenant la ressource. Apache fournit ensuite la ressource, dans notre exemple, la page `index.html`, au client. Dans ce cas, le fichier se trouve dans le répertoire de niveau supérieur. Toutefois, les ressources peuvent également se trouver dans des sous-répertoires, comme dans `http://www.example.com/linux/novell/suse`.

46.1.4 Directive

Pour configurer Apache, le terme *directive* est souvent utilisé comme synonyme d'« option de configuration. » Directive est le terme technique relatif au logiciel serveur Web Apache.

46.2 Installation

Apache sur SUSE Linux s'exécute "prêt à utiliser" avec une configuration standard prédéfinie. En suivant les instructions de ce chapitre, vous pouvez mettre en service le serveur Web Apache en peu de temps. Vous devez être un utilisateur `root` pour installer et configurer Apache.

46.2.1 Installation d'Apache avec YaST

Le système de fichiers et la disposition des applications du paquetage SUSE Linux apache2 sont légèrement différents de ceux des paquetages logiciels standard disponibles sur le site Web d'Apache (`http://httpd.apache.org`). La section suivante décrit précisément l'installation du paquetage SUSE Linux apache2 et indique les différences, si nécessaire.

Pour installer un serveur Web simple, procédez comme suit :

Procédure 46.1 *Installation rapide*

1 Démarrez YaST dans l'interface graphique ou en mode ligne de commande.

2 Sélectionnez *Services réseau* → *Serveur HTTP*.

3 Cliquez sur *Continuer* pour confirmer l'installation des paquetages `apache2` et `apache2-prefork`.

4 Lorsque l'installation est terminée, l'*assistant de configuration d'Apache* apparaît et vous pouvez alors commencer la configuration du serveur Web.

L'inconvénient de la procédure mentionnée ci-dessus est qu'il n'y a pas de prise en charge PHP, ni de la base de données. Pour installer un serveur Web avec prise en charge PHP et prise en charge de la base de données, procédez comme suit :

Procédure 46.2 *Installation d'un serveur Web simple*

1 Démarrez YaST dans l'interface graphique ou en mode ligne de commande.

2 Sélectionnez *Logiciels* → *Installer et supprimer des logiciels*.

3 Choisissez *Sélections* dans la zone *Filtre*, puis activez l'option *Serveur Web simple avec Apache2*.

4 Cliquez sur *OK*.

5 Confirmez l'installation des paquetages dépendants pour achever l'installation de SUSE Linux Apache2.

Pour les utilisateurs experts, SUSE Linux offre une option d'installation personnalisée du paquetage. Pour installer un serveur Web de manière personnalisée, procédez comme suit :

Procédure 46.3 *Installation du RPM Apache par défaut avec YaST*

1. Démarrez YaST dans l'interface graphique ou en mode ligne de commande. Sélectionnez *Logiciels* → *Installer et supprimer des logiciels*.

2. Dans *Filtre*, sélectionnez *Recherche*, puis entrez `apache2` dans le champ de *recherche*.

3. Sélectionnez `apache2` pour l'installation.

4. Utilisez les étapes 2 et 3 pour la sélection des modules. (voir Section 46.5, « Modules Apache » (p. 767)).

5. Une fois la sélection effectuée, cliquez sur *Accepter*.

6. Vous êtes alors invité à choisir l'une des dépendances pour le paquetage `apache2-MPM` nécessaire : `apache2-prefork` ou `apache2-worker`. Consultez laSection 46.2.2, « Modules de multitraitement » (p. 741) pour connaître les différences qui les distinguent. En cas de doute, sélectionnez le paquetage `apache2-prefork`, paquetage par défaut des systèmes d'exploitation basés sur Unix, puis cliquez sur *OK*.

7. Confirmez l'installation des paquetages dépendants pour achever l'installation de SUSE Linux Apache2.

REMARQUE: Démarrage d'un serveur Web

L'installation d'Apache ne démarre pas le serveur Web automatiquement. Pour plus d'informations sur le contrôle du démarrage et de l'arrêt d'Apache, consultez la Section 46.3.3, « Activation, démarrage et arrêt d'Apache » (p. 761).

46.2.2 Modules de multitraitement

Comme indiqué dans Installation du RPM Apache par défaut avec YaST (p. 741), SUSE Linux offre deux modules de multitraitement différents (MPM) utilisables avec Apache.

Le rôle des MPM est d'accepter et de gérer les requêtes au serveur Web. Ils représentent le noyau du logiciel serveur Web.

Module prefork MPM

Les modules prefork MPM implémentent un serveur Web preforking sans thread. De ce fait, le serveur Web se comporte de façon semblable à la version 1.x d'Apache en ce qu'il isole chaque requête et la gère en dupliquant un processus enfant séparé. Ainsi les requêtes problématiques n'ont-elles pas d'incidence sur les autres, ce qui évite de verrouiller le serveur Web.

Tout en apportant de la stabilité avec cette approche basée sur les processus, le module prefork MPM consomme davantage de ressources système que son équivalent, le module worker MPM. Le module prefork MPM est considéré comme le MPM par défaut pour les systèmes d'exploitation de type Unix.

IMPORTANT: Les MPM dans ce document

Ce document suppose qu'Apache est utilisé avec le module prefork MPM.

Module worker MPM

Le module worker MPM offre un serveur Web multithread. Un thread est une forme « plus légère » de processus. L'avantage d'un thread sur un processus tient à sa plus faible consommation de ressources. Plutôt que de ne dupliquer que les processus enfants, le module worker MPM sert les requêtes en utilisant des threads avec des processus serveur. Les processus enfant pré-dupliqués sont multithread.

Cette approche améliore les performances d'Apache en consommant moins de ressources système que le module prefork MPM. L'un des inconvénients majeurs est la stabilité du module worker MPM : si un thread est endommagé, tous les threads d'un processus peuvent être affectés. Dans le pire des cas, il peut en résulter le blocage du serveur. En particulier, lorsqu'on utilise CGI (décrit dans la section intitulée « Common Gateway Interface : `mod_cgi` » (p. 769)) avec Apache sous une charge importante, des erreurs internes du serveur peuvent se produire du fait que des threads ne peuvent communiquer avec les ressources système.

Un autre argument en défaveur de l'utilisation du module worker MPM avec Apache est que tous les modules Apache disponibles (voir Section 46.5, « Modules Apache »

(p. 767)) ne sont pas thread-safe et ne peuvent donc pas être utilisé conjointement avec ce module.

AVERTISSEMENT: PHP en tant que module Apache (mod_php)

Tous les modules PHP disponibles ne sont pas thread-safe. L'utilisation du module worker MPM avec `mod_php` est vivement déconseillée.

46.2.3 Système de fichiers et configuration d'application par défaut

SUSE Linux place les fichiers du paquetage Apache dans des emplacements par défaut. Les emplacements des fichiers les plus importants sont indiqués ici.

Fichiers binaires

La plupart des fichiers exécutables de SUSE Linux Apache sont accompagnés d'un `2`. Ceci simplifie la différenciation des fichiers binaires pour l'installation parallèle d'Apache 1.x et d'Apache 2.x.

/usr/sbin/httpd2
: Lien symbolique pointant vers le module de multitraitement choisi décrit dans Section 46.2.2, « Modules de multitraitement » (p. 741). La valeur par défaut est `httpd2-prefork`. Le lien symbolique est géré par le script de démarrage conformément au paramètre de configuration système du MPM.

/usr/sbin/httpd2-prefork
: L'exécutable Apache2.

/usr/sbin/apache2ctl
: Script de contrôle pour démarrer et arrêter le serveur Web, fourni par le projet Apache HTTPD. Consultez Section 46.3.3, « Activation, démarrage et arrêt d'Apache » (p. 761) pour plus d'informations ou exécutez `/usr/sbin/apache2ctl help`.

/etc/init.d/apache2
: Script de démarrage et d'arrêt offrant l'intégration complète dans l'installation de SUSE Linux et démarrant Apache lors de l'amorçage. Il vérifie la présence d'une

configuration valide avant de démarrer et d'arrêter le serveur et remplace l'emplacement de la configuration. Il facilite l'inclusion d'autres fichiers de configuration, le chargement de modules, ou même le démarrage d'une instance séparée du serveur sans modification du script.

/usr/sbin/rcapache2
: Un lien symbolique pour `/etc/init.d/apache2`, car `/etc/init.d/` n'est pas le chemin par défaut. Utilisez simplement `rcapache2 start` pour démarrer Apache.

/usr/sbin/htpasswd2
: Utilitaire permettant de générer des mots de passe codés pour l'authentification basée sur `.htaccess`. Reportez-vous à la page de manuel `htpasswd2(1)` pour plus de détails sur l'utilisation de cet utilitaire.

Fichiers de configuration

La plupart des fichiers de configuration résident sous `/etc/apache2`. Pour plus d'informations sur la modification des paramètres de configuration, consultez Section 46.3, « Configuration » (p. 747).

/etc/apache2/httpd.conf
: Fichier de configuration de niveau supérieur. Si possible, évitez de modifier ce fichier. Il inclut principalement d'autres fichiers de configuration et déclare les paramètres généraux.

/etc/apache2/*.conf
: Certains modules externes Apache placent leurs fichiers de configuration dans le répertoire `/etc/apache2/`, généralement précédés par le nom du module lui-même (`mod_*.conf`).

/etc/apache2/conf.d/*
: Répertoire contenant plusieurs autres fichiers de configuration qui accompagnent certains paquetages. Pour voir un exemple, consultez la section intitulée « Service de PHP : `mod_php4`, `mod_php5` » (p. 776).

/etc/apache2/vhosts.d/*
: Répertoire contenant les fichiers de configuration facultatifs pour les hôtes virtuels. Pour plus de détails, reportez-vous à Section 46.4, « Hôtes virtuels » (p. 763).

/etc/sysconfig/apache2

Fichier de configuration SUSE Linux associé à Apache2. Il contient tous les paramètres de configuration pertinents pour contrôler le serveur Web Apache. `/etc/sysconfig/apache2` est utilisé par YaST pour configurer Apache comme décrit dans Section 46.3.1, « Configuration d'Apache avec YaST » (p. 747). Il est également possible de le modifier manuellement comme décrit dans Section 46.3.2, « Configuration manuelle d'Apache » (p. 754).

Fichiers journaux

Par défaut, Apache fournit différentes informations concernant son état lors de l'exécution dans les fichiers suivants :

/var/log/apache2/error_log

Apache consigne les avertissements de démarrage et d'arrêt ainsi que toutes les erreurs d'exécution dans ce fichier.

/var/log/apache2/access_log

Toutes les requêtes vers le serveur Web sont enregistrées dans ce fichier. Le format par défaut des entrées est un format combiné, montrant des informations concernant l'hôte et l'agent utilisateur envoyant la requête et l'URI de référence.

Racine du document

Le répertoire physique `/srv/www/htdocs` est l'emplacement par défaut à partir duquel Apache sert les pages Web. Il agit comme « répertoire racine » pour une requête du client. Pour publier des pages Web avec Apache, stockez les fichiers de façon hiérarchique dans ou sous ce répertoire.

Une URL telle que http://www.example.com/index.html se réfère à `/srv/www/htdocs/index.html` dans la configuration Apache par défaut de SUSE Linux pour un domaine nommé example.com.

46.2.4 Création manuelle de modules

Apache a été conçu avec une approche modulaire, ce qui signifie que les modules offrent les possibilités du logiciel serveur Web lui-même. Par conséquent, Apache peut être enrichi par des utilisateurs avancés en écrivant des modules personnalisés. Reportez-

vous aux pages de manuel mentionnées ci-dessous pour obtenir des informations plus détaillées.

apache2-devel

Pour pouvoir développer des modules pour Apache ou compiler des modules tiers, le paquetage `apache2-devel` est nécessaire, ainsi que les outils de développement correspondants. `apache2-devel` contient également les outils `apxs2`, nécessaires pour compiler des modules supplémentaires pour Apache.

apxs2

Les fichiers binaires `apxs2` se trouvent sous `/usr/sbin` :

- `/usr/sbin/apxs2`—permet de créer un module d'extension fonctionnant avec n'importe quel MPM. L'emplacement d'installation est `/usr/lib/apache2`.
- `/usr/sbin/apxs2-prefork`—adapté aux modules prefork MPM. L'emplacement d'installation est `/usr/lib/apache2-prefork`.
- `/usr/sbin/apxs2-worker`—adapté aux modules worker MPM.

`apxs2` installe les modules pour les rendre utilisables pour tous les MPM. Les deux autres programmes installent les modules afin qu'ils soient utilisables seulement pour leurs MPM respectifs. `apxs2` installe les modules dans `/usr/lib/apache2` et `apxs2-prefork` installe les modules dans `/usr/lib/apache2-prefork`.

`apxs2` permet la compilation et l'installation des modules à partir du code source (avec les modifications requises des fichiers de configuration), qui crée des *objets partagés de façon dynamique* (DSO - dynamic shared object) pouvant être chargés dans Apache lors de l'exécution. Installez un module à partir du code source avec les commandes `cd /path/to/module/source; apxs2 -c -i mod_foo.c`. D'autres options de `apxs2` sont décrites dans la page de manuel `apxs2(1)`. Les modules doivent être activés dans `/etc/sysconfig/apache2` avec l'entrée `APACHE_MODULES` comme décrit dans Section 46.3.2, « Configuration manuelle d'Apache » (p. 754).

46.3 Configuration

Apache dans SUSE Linux peut être configuré de deux façons différentes : avec YaST ou manuellement. La configuration manuelle offre un niveau de détail supérieur, mais est moins pratique que l'interface utilisateur graphique de YaST.

IMPORTANT: Modifications de configuration

La modification de certaines valeurs de configuration d'Apache ne prend effet qu'après le redémarrage d'Apache. Ceci se produit automatiquement lorsque vous terminez la configuration avec YaST et que l'option *Activé* du *Service HTTP* est sélectionnée. Le redémarrage manuel est décrit dans la Section 46.3.3, « Activation, démarrage et arrêt d'Apache » (p. 761). La plupart des modifications de configuration ne nécessitent qu'un rechargement avec `rcapache2 reload`.

46.3.1 Configuration d'Apache avec YaST

YaST vous permet de transformer un hôte de votre réseau en serveur Web. Pour configurer un tel serveur, démarrez YaST et sélectionnez *Services réseau* → *Serveur HTTP*. Lorsque vous lancez ce module pour la première fois, l'assistant (wizard) serveur HTTP démarre et vous invite à prendre quelques décisions de base concernant l'administration du serveur.

Assistant (wizard) serveur HTTP

L'assistant (wizard) serveur HTTP comprend cinq étapes ou boîtes de dialogue. Dans la dernière boîte de dialogue, vous pouvez passer en mode de configuration pour experts afin d'effectuer des paramétrages encore plus pointus.

Sélection du périphérique réseau

Spécifiez les interfaces réseau et les ports qu'Apache utilise pour écouter les requêtes entrantes. Vous pouvez sélectionner toute combinaison d'interfaces réseau existantes et leurs adresses IP respectives. Vous pouvez utiliser les ports de ces trois plages (ports connus, ports enregistrés et ports dynamiques ou privés) qui ne sont pas réservés par d'autres services.

Le paramètre par défaut est l'écoute sur toutes les interfaces réseau (adresses IP) sur le port 80. Lorsque le pare-feu est activé, vous pouvez vérifier si vous devez y activer les ports Apache.

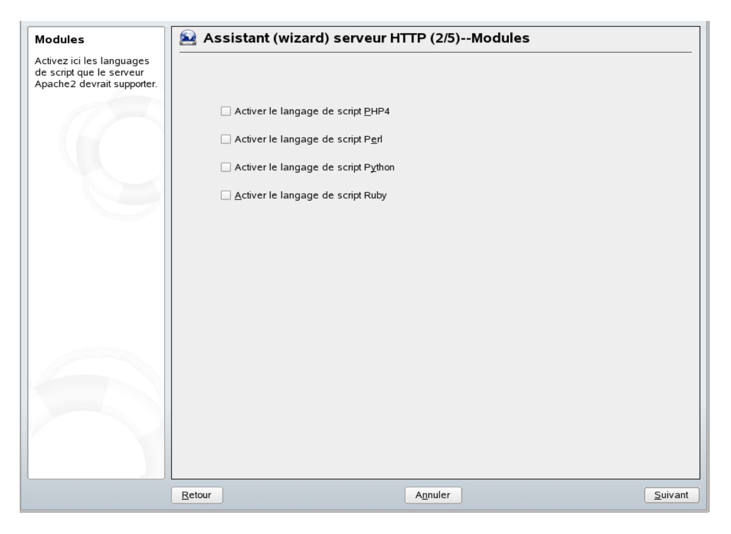
Cochez la case *Ouvrir le pare-feu sur les ports sélectionnés* pour ouvrir les ports dans le pare-feu sur lequel le serveur Web procède à l'écoute. Cette opération est nécessaire pour rendre le serveur Web disponible sur le réseau, qui peut être un réseau local, étendu ou le réseau Internet public. Il est utile de maintenir fermé le port `Listen` dans les situations de test où aucun accès extérieur au serveur Web n'est nécessaire. Si les paramètres par défaut vous conviennent ou si avez effectué des modifications, cliquez sur *Suivant* pour poursuivre la configuration.

Figure 46.1 *Assistant (wizard) serveur HTTP : Sélection du périphérique réseau*

Modules

Le paquetage SUSE Linux Apache est fourni avec de nombreux modules Apache. Ces modules étendent les fonctionnalités d'Apache et sont disponibles pour une vaste gamme de tâches. L'option de configuration *Modules* permet le chargement et le déchargement de divers modules Apache au moment du démarrage du serveur. Pour une explication plus détaillée des modules, consultez la Section 46.5, « Modules Apache » (p. 767). Cliquez sur *Suivant* pour continuer.

Figure 46.2 *Assistant (wizard) serveur HTTP : Modules*



Hôte par défaut

Cette option concerne le serveur Web par défaut. Comme l'explique la Section 46.4, « Hôtes virtuels » (p. 763), Apache peut servir plusieurs domaines à partir d'une seule machine physique. Le premier domaine déclaré (ou `VirtualHost`) du fichier de configuration est généralement appelé *hôte par défaut*. Pour modifier les paramètres de l'hôte, choisissez l'entrée correspondante dans le tableau, puis cliquez sur *Modifier*. Pour ajouter un hôte supplémentaire, cliquez sur *Ajouter*. Pour supprimer un hôte, sélectionnez-le et cliquez sur *Supprimer*.

À cette étape, vous pouvez ajouter une option et une valeur SSL (Secure Sockets Layer) aux paramètres de l'hôte. Pour plus d'informations à ce sujet, consultez la section intitulée « Ajout de la prise en charge SSL » (p. 754).

Figure 46.3 *Assistant (wizard) serveur HTTP : Hôte par défaut*

Vous trouverez ci-dessous la liste des paramètres par défaut du serveur :

Document Root

Comme l'explique la section intitulée « Racine du document » (p. 745), `/srv/www/htdocs` est l'emplacement par défaut à partir duquel Apache diffuse des pages Web.

Répertoire

`/srv/www/htdocs` est l'emplacement des pages Web.

Alias

À l'aide des directives `Alias`, les URL peuvent être assignées à des emplacements physiques du système de fichiers. Par conséquent, vous pouvez accéder à un chemin particulier même *en dehors* de `Document Root` dans le système de fichiers par l'intermédiaire d'une URL avec un alias sur ce chemin.

L'`alias /icons` SUSE Linux par défaut pointe vers `/usr/share/apache2/icons` pour les icônes Apache affichées dans la vue d'index de répertoire.

Répertoire

`/usr/shareapache2/icons` est l'emplacement du répertoire `Alias`.

ScriptAlias
Comme la directive `Alias`, la directive `ScriptAlias` assigne une URL à un emplacement de système de fichiers. La différence est que `ScriptAlias` désigne le répertoire cible comme un emplacement CGI, c'est-à-dire que les scripts CGI doivent être exécutés à cet emplacement.

Répertoire
`/srv/www/cgi-bin` est l'emplacement du répertoire `ScriptAlias`.

Include
`/etc/apache2/conf.d/*.conf` est le répertoire qui contient les fichiers de configuration fournis avec certains paquetages. `/etc/apache2/conf.d/apache2-manual?conf` est le répertoire qui contient tous les fichiers de configuration `apache2-manual`.

Résolution du serveur
Cette option fait référence à la Section 46.4, « Hôtes virtuels » (p. 763).

Déterminer le serveur de requête par des en-têtes HTTP permet à un `VirtualHost` de répondre à une requête sur son nom de serveur (consultez la Section 46.4.1, « Hôtes virtuels à base de nom » (p. 763)).

Déterminer le serveur de requête par l'adresse IP du serveur permet à Apache de sélectionner l'hôte demandé par les informations d'en-tête HTTP que le client envoie. Consultez la Section 46.4.2, « Hôtes virtuels à base d'adresse IP » (p. 766) pour plus d'informations sur les hôtes virtuels basés sur IP.

Nom du serveur
Cette option indique l'URL par défaut utilisée par les clients pour contacter le serveur Web. Utilisez un nom de domaine complet (consultez Domaine (p. 738)) pour atteindre le serveur Web à l'adresse `http://`*`nom de domaine complet`* ou son adresse IP.

Courrier électronique de l'administrateur du serveur
Fournit l'adresse électronique de l'administrateur du serveur Web pour cette option.

Après avoir terminé l'étape *Hôte par défaut*, cliquez sur *Suivant* pour poursuivre avec la boîte de dialogue de configuration.

Hôtes virtuels

À cette étape, l'assistant affiche la liste des hôtes virtuels déjà configurés (consultez la Section 46.4, « Hôtes virtuels » (p. 763)). L'un des hôtes est identifié comme étant celui par défaut (par un astérisque en regard du nom du serveur). Pour définir un hôte par défaut, sélectionnez le serveur et cliquez sur *Défini par défaut*.

Pour ajouter un hôte, cliquez sur *Ajouter* pour ouvrir la boîte de dialogue qui permet d'entrer les informations de base concernant cet hôte. La zone *Identification du serveur* comprend le nom du serveur, la racine de contenu du serveur et le courrier électronique de l'administrateur. Le texte d'aide dans le cadre situé à gauche de la fenêtre explique chacun de ces éléments en détail. L'option *Résolution du serveur* est utilisée pour déterminer le mode d'identification d'un hôte. Vous pouvez indiquer si vous souhaitez déterminer un serveur de requête à partir des en-têtes HTTP ou par l'adresse IP du serveur en sélectionnant l'option correspondante. L'autre méthode consiste à déterminer l'hôte virtuel par l'adresse IP utilisée par le client lors de la connexion au serveur. Vous pouvez également activer la prise en charge SSL en cochant cette case. Vous pouvez aussi spécifier le chemin du fichier de certificat. Cliquez sur *Parcourir* pour afficher le répertoire par défaut `/etc/apache2/ssl.crt`. Après avoir entré toutes les informations, cliquez sur *Suivant* pour passer à la dernière étape de configuration.

Figure 46.4 *Assistant (wizard) serveur HTTP : Hôtes virtuels*

Résumé

Il s'agit de la dernière étape de l'assistant. Indiquez-y le mode et le moment de démarrage du serveur Apache, à savoir lors de l'amorçage ou manuellement. Le port sélectionné précédemment s'affiche également, ainsi que les hôtes par défaut et virtuels. Si ces paramètres vous conviennent, cliquez sur *Terminer* pour achever la configuration.

Figure 46.5 *Assistant (wizard) serveur HTTP : Résumé*

Configuration du serveur HTTP pour experts

Le module Serveur HTTP vous permet également d'affiner davantage la configuration. Cliquez sur *Configuration du serveur HTTP pour experts* pour obtenir des options de configuration supplémentaires. Vous pouvez alors effectuer les modifications suivantes :

Écouter

Sélectionnez *Écouter* et cliquez sur *Modifier* pour ouvrir une nouvelle fenêtre dans laquelle vous pouvez ajouter, supprimer ou modifier des entrées.

Modules

Sélectionnez *Modules* et cliquez sur *Modifier* pour pouvoir modifier l'état des modules Apache2 en cliquant sur *État de l'interrupteur à bascule*. Cliquez sur *Ajouter un module* pour ajouter un nouveau module.

Hôte par défaut
Sélectionnez *Hôte par défaut* et cliquez sur *Modifier* pour pouvoir modifier les paramètres de l'hôte. Vous pouvez également ajouter, modifier ou supprimer des options.

Hôtes
Sélectionnez *Hôtes* et cliquez sur *Modifier* pour pouvoir ajouter, supprimer, modifier ou sélectionner un hôte par défaut.

Dans toutes les boîtes de dialogue précédentes, vous pouvez cliquer sur *Fichiers de journalisation* pour consulter le journal d'erreurs et le journal d'accès. Cliquez sur *OK* pour achever la configuration et revenir au centre de contrôle YaST.

Ajout de la prise en charge SSL

Pour ajouter une option SSL à l'hôte, cliquez sur *Ajouter* à la troisième étape (hôte par défaut) de l'assistant (wizard) serveur HTTP. Si votre serveur a déjà été configuré et que vous n'avez plus accès à l'assistant, vous pouvez configurer une option SSL en sélectionnant *Hôte par défaut* dans la boîte de dialogue Configuration du serveur HTTP ou en cliquant sur *Modifier*, puis sur *Ajouter*. Dans ces deux cas, la fenêtre contextuelle qui apparaît vous permet de sélectionner une option *SSL* et de la confirmer en cliquant sur *OK*. Vous êtes ensuite invité à entrer la valeur de l'option sélectionnée. Cette opération peut se limiter à l'*activation* ou à la *désactivation* de l'option, mais il arrive que vous deviez entrer la valeur appropriée. En cas de doute, consultez la documentation sur les paramètres de valeur lors de la configuration SSL. Dès que vous cliquez sur *OK*, l'option et la valeur apparaissent dans la liste de configuration de l'hôte. Cliquez sur *Suivant* pour accéder à l'étape suivante de la boîte de dialogue de configuration.

Si l'option *SSL* apparaît dans la liste de configuration de l'hôte, cliquez sur *Modifier* pour ouvrir la boîte de dialogue de configuration correspondante. Sinon, cliquez sur *Ajouter*, sélectionnez *SSL*, puis cliquez sur *OK*. La boîte de dialogue s'ouvre alors automatiquement. Vous pouvez ainsi ajouter, supprimer ou modifier des options SSL. Cliquez sur *OK* pour revenir à l'assistant (wizard) serveur HTTP.

46.3.2 Configuration manuelle d'Apache

La configuration manuelle d'Apache implique la modification des fichiers de configuration en texte brut en tant qu'utilisateur `root`.

IMPORTANT: Pas de module SUSEconfig pour Apache2

Le module SUSEconfig pour Apache2 a été retiré de SUSE Linux. Il n'est plus nécessaire d'exécuter `SUSEconfig` après avoir modifié `/etc/sysconfig/apache2`.

/etc/sysconfig/apache2

`/etc/sysconfig/apache2` contrôle certains paramètres généraux d'Apache, tels que les modules à charger, les fichiers de configuration supplémentaires à inclure, les drapeaux avec lesquels on doit démarrer le serveur et ceux qui doivent être ajoutés à la ligne de commande. Chaque option de configuration de ce fichier est très documentée et n'est donc pas mentionnée ici. Pour un serveur Web d'utilité générale, `/etc/sysconfig/apache2` doit suffire à tous les besoins de configuration. Pour les configurations spécifiques, reportez-vous à la section intitulée « Directives Apache dans /etc/apache2/httpd.conf: Environnement global » (p. 756).

IMPORTANT: Fichiers créés automatiquement au démarrage du serveur

`/etc/sysconfig/apache2` crée ou modifie automatiquement les fichiers suivants lors du démarrage ou du redémarrage du serveur Web.

- `/etc/apache2/sysconfig.d/loadmodule.conf`—modules chargés lors de l'exécution
- `/etc/apache2/sysconfig.d/global.conf`—paramètres généraux pour l'ensemble du serveur
- `/etc/apache2/sysconfig.d/include.conf`—liste des fichiers de configuration inclus

Ne modifiez pas ces fichiers manuellement. Modifiez plutôt les paramètres correspondants dans `/etc/sysconfig/apache2`.

Pour peaufiner la configuration, consultez les fichiers qui se trouvent dans `/etc/apache2/*`, en particulier pour les modifications de configuration manuelles apportées aux hôtes virtuels, à l'environnement global ou au serveur principal.

Directives Apache dans /etc/apache2/httpd.conf: Environnement global

SUSE Linux utilise `/etc/apache2/httpd.conf` comme point central de référence pour d'autres fichiers de configuration. Ne modifiez le fichier que pour activer les fonctions qui ne sont pas disponibles dans `/etc/sysconfig/apache2`. Les directives de la section *Environnement global* de `httpd.conf` concernent le fonctionnement global d'Apache.

Les sections qui suivent décrivent certaines des directives qui ne sont pas disponibles dans YaST. Les principales directives telles que `Document Root` (Document Root (p. 750)) sont essentielles et requises dans l'`Environnement global` et pour l'`hôte virtuel`.

Les paramètres et directives suivants sont classés par affiliation logique et domaine de configuration. Ils doivent être définis dans `/etc/apache2/httpd.conf`.

`LoadModule` ***`identificateur_module /chemin/vers/module`***

La directive `LoadModule` spécifie un module Apache à charger lors de l'exécution. *`identificateur_module`* est le nom du module dans sa documentation. *`/chemin/vers/module`* peut être un chemin absolu ou relatif pointant vers le fichier.

Exemple 46.1 *Directive LoadModule*

```
LoadModule rewrite_module /usr/lib/apache2-prefork/mod_rewrite.so
```

Sur SUSE Linux, il n'est pas nécessaire d'utiliser des instructions `LoadModule` directement. À la place, `APACHE_MODULE` est utilisé dans `/etc/sysconfig/apache2`.

`MaxClients` ***`nombre`***

Le nombre maximal de clients qu'Apache peut gérer simultanément. MaxClients doit être suffisamment grand pour gérer autant de requêtes simultanées que le site Web s'attend à en recevoir, mais suffisamment petit pour garantir que la RAM physique est suffisante pour tous les processus.

`Timeout` ***`secondes`***

Spécifie la durée d'attente avant qu'Apache ne signale un dépassement de délai pour une requête.

Directives Apache dans /etc/apache2/httpd.conf: Serveur principal

Les directives de la section `Serveur principal` s'appliquent lorsque des requêtes du client ne sont pas gérées par un `Hôte virtuel` et doivent donc être traitées par un serveur par défaut ou principal. En outre, les paramètres définis dans ce contexte sont les paramètres par défaut pour tous les hôtes virtuels configurés. Il en résulte que toutes les directives du `serveur principal` peuvent également être définies dans le contexte `Hôte virtuel`, et remplacent les paramètres par défaut.

`noms de fichier` **`DirectoryIndex`**

Définissez les fichiers qu'Apache doit rechercher pour terminer une adresse URL sans spécification de fichier. Le paramètre par défaut est `index.html`. Par exemple, si le client demande l'adresse URL `http://www.example.com/foo/` et si le répertoire`foo` contient un fichier nommé `index.html`, Apache transmet cette page au client. Pour déclarer plusieurs files, séparez-les par des espaces.

Exemple 46.2 *Directive DirectoryIndex*

```
DirectoryIndex index.html index.shtml start.php begin.pl
```

`AllowOverride` **`Toutes | Aucune |`** ***`option`***

Cette directive peut s'utiliser *uniquement* à l'intérieur d'une déclaration `<Répertoire></Répertoire>`. (voir Répertoire (p. 750)).

`AllowOverride` spécifie les options d'accès et d'affichage qu'un fichier `.htaccess` (ou d'autres fichiers spécifiés par `AccessFileName` décrits dans la section intitulée « *`noms de fichier`* `AccessFileName` » (p. 759)) peut remplacer.

Les valeurs possibles sont :

Toutes
: Toutes les options peuvent être remplacées par un fichier `.htaccess`.

Aucune
: Aucune option ne peut être remplacée par un fichier `.htaccess`.

AuthConfig
: Les répertoires peuvent être protégés par mot de passe à l'aide d'un fichier `.htaccess`.

FileInfo
: Permet l'utilisation de directives contrôlant les types de document au sein d'un fichier `.htaccess`. Un exemple classique consiste à configurer des pages d'erreur personnalisées avec `ErrorDocument` (voir http://httpd.apache.org/docs-2.0/mod/core.html#errordocument).

Indexes
: Dans le cas où aucun document `DirectoryIndex` n'a été trouvé, ce paramètre permet à Apache de contrôler l'affichage du contenu du répertoire.

Limit
: Contrôle l'accès à un répertoire ou à certains fichiers pour les clients. Les directives `Allow`, `Deny` et `Order` sont utilisées à cette fin au sein d'un fichier `.htaccess`. Pour connaître l'utilisation de ces directives, consultez la documentation du module d'accès (http://httpd.apache.org/docs-2.0/mod/mod_access.html).

Options
: Permet l'utilisation des directives `Options` et `XBitHack` au sein d'un fichier `.htaccess`. La directive `Options` (http://httpd.apache.org/docs-2.0/mod/core.html#options) contrôle les fonctions du serveur qui sont disponibles dans un répertoire particulier. La directive `XBitHack` (http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack) permet aux fichiers dont l'octet execute est défini pour être analysé en tant que SSI (voir la section intitulée « Inclusions côté serveur avec `mod_include` » (p. 768)).

IMPORTANT

Ces paramètres sont appliqués de façon récurrente au répertoire actuel et à ses sous-répertoires. Ces options, excepté `Toutes` et `Aucune`, peuvent être combinées en les séparant par des espaces.

***Exemple 46.3** Directive AllowOverride*

```
<Directory /srv/www/htdocs>
 AllowOverride None
</Directory>
<Directory /srv/www/htdocs/project>
 AllowOverride All
</Directory>
<Directory /srv/www/htdocs/project/webapp>
 AllowOverride Indexes Limit AuthConfig
</Directory>
```

noms de fichier AccessFileName

`AccessFileName` définit le nom des fichiers qui peuvent remplacer les permissions d'accès globales et d'autres paramètres des répertoires (voir Répertoire (p. 750)).

Le paramètre par défaut est `.htaccess`. Pour déclarer plusieurs files, séparez-les par des espaces.

***Exemple 46.4** Directive AccessFileName*

```
AccessFileName .htaccess .acl permission.txt
```

ErrorLog *fichier | "|commande"*

Spécifie le nom du fichier dans lequel Apache consigne les messages d'erreur. Apache peut également effectuer la consignation dans une commande ou un script. Le paramètre par défaut `/var/log/apache2/error_log`.

***Exemple 46.5** Directive ErrorLog*

```
ErrorLog /var/log/apache2/error_log
ErrorLog "|/path/to/script"
```

niveau LogLevel

Ceci définit le niveau de commentaires des messages du journal à enregistrer. Par ordre croissant de niveau de commentaires (et par ordre décroissant de gravité des messages), *le niveau* peut être

- emerg
- alert
- crit
- error
- warn
- notice
- info
- debug

Le paramètre par défaut est warn. Il est recommandé pour l'utilisation quotidienne. Pour des utilisations de débogage, info et debug apportent des informations utiles.

Exemple 46.6 *Directive LogLevel*

```
LogLevel debug
```

Directives Apache dans /etc/apache2/httpd.conf: Section Hôtes virtuels

Pour gérer plusieurs domaines ou noms d'hôte sur une machine physique, des conteneurs Hôte virtuel sont nécessaires. Ils sont déclarés dans les sections Hôtes virtuels de la configuration. Pour plus de détails sur la syntaxe et les fonctionnalités des hôtes virtuels, reportez-vous à Section 46.4, « Hôtes virtuels » (p. 763).

46.3.3 Activation, démarrage et arrêt d'Apache

Pour activer le serveur Web Apache au démarrage, utilisez l'éditeur de niveau d'exécution de YaST. Pour le démarrer, sélectionnez *Système* → *Services système (niveau d'exécution)* dans YaST. Naviguez ensuite jusqu'à l'entrée *apache2*. Choisissez *Activer* pour qu'Apache démarre automatiquement lors de l'amorçage de la machine. Les personnes expérimentées peuvent utiliser l'outil `chkconfig` pour obtenir la même chose sur la ligne de commande : `/sbin/chkconfig -a apache2`.

Pour démarrer ou arrêter Apache, utilisez le script `/usr/sbin/rcapache2` en tant qu'utilisateur `root`. `/usr/sbin/rcapache2` prend les paramètres suivants pour démarrer et arrêter le serveur Web Apache :

`start`
: Démarre le serveur Web Apache.

`startssl`
: Démarre le serveur Web Apache avec le support SSL. Pour plus d'informations sur la configuration d'Apache avec SSL, reportez-vous à la section intitulée « Ajout de la prise en charge SSL » (p. 754) et à la section intitulée « Secure Sockets Layer et Apache : `mod_ssl` » (p. 773).

`stop`
: Arrête le serveur Web Apache.

`configtest`
: Teste la configuration Apache sans arrêter, démarrer ou redémarrer le serveur Web. Du fait que ce test est forcé chaque fois que le serveur est démarré, rechargé ou redémarré, il n'est généralement pas nécessaire de l'exécuter de façon explicite.

`restart`
: Arrête, puis redémarre le serveur Web.

`try-restart`
: Redémarre le serveur Web s'il fonctionne.

`restart-hup`
Redémarre le serveur Web Apache en lui envoyant un signal `SIGHUP`. Normalement, ceci n'est pas utilisé.

`graceful` et **`reload`**
Arrête le serveur Web en conseillant à tous les processus Apache dupliqués de terminer leur requête avant de se fermer. À mesure qu'un processus disparaît, il est remplacé par un qui vient d'être démarré, ce qui se traduit par le "redémarrage" complet d'Apache.

ASTUCE

`rcapache2 reload` est la méthode privilégiée de redémarrage d'Apache dans les environnements de production, car il permet à tous les clients d'être servis sans provoquer de ruptures de connexion.

`status`
Vérifie l'état lors de l'exécution du serveur Web Apache.

Exemple 46.7 *Exemple de résultat lors du démarrage et de l'arrêt d'Apache*

```
tux@sun # rcapache2 status
Checking for httpd2:                                       unused

tux@sun # rcapache2 configtest
Syntax OK

tux@sun # rcapache2 start
Starting httpd2 (prefork)                                  done

tux@sun # rcapache2 status
Checking for httpd2:                                       running

tux@sun # rcapache2 graceful
Reload httpd2 (graceful restart)                           done

tux@sun # rcapache2 status
Checking for httpd2:                                       running
```

Un fichier de configuration incorrect peut se traduire par le démarrage incorrect d'Apache ou par son absence de démarrage. En l'absence de démarrage, il se peut qu'aucun message ne s'affiche. Consultez toujours le journal d'erreur principal pour chaque démarrage et redémarrage.

46.4 Hôtes virtuels

Le terme *hôte virtuel* se réfère à la possibilité d'Apache de servir plusieurs URI (identificateurs de ressources universels) à partir de la même machine physique. Cela signifie que plusieurs domaines, tels que www.example.com et www.exemple.net, sont exécutés par un même serveur Web sur une seule machine physique.

Il est courant d'utiliser des hôtes virtuels pour économiser les ressources administratives (un seul serveur Web à gérer) et les dépenses en matériel (chaque domaine n'a pas besoin d'un serveur dédié). Les hôtes virtuels peuvent être basés sur le nom, sur l'adresse IP ou sur le port.

Les hôtes virtuels peuvent être configurés via YaST (voir Hôte par défaut (p. 749)) ou en modifiant manuellement la section `Hôte virtuel` du fichier `httpd.conf` (voir Section 46.3.2, « Configuration manuelle d'Apache » (p. 754)).

Par défaut, Apache dans SUSE Linux est préparé pour un fichier de configuration par hôte virtuel dans `/etc/apache2/vhosts.d/`. Un modèle de base pour un hôte virtuel est fourni dans ce répertoire (`vhost.template`). La configuration d'un hôte virtuel peut également s'ajouter ailleurs, par exemple dans un fichier inclus à la configuration.

IMPORTANT

Il est très utile de vérifier la configuration de l'hôte virtuel à l'aide de la commande `httpd2 -S`. Cela indique les paramètres de l'hôte virtuel tels qu'ils sont interprétés par Apache et peut vous aider à vérifier que vous obtenez les résultats escomptés. Si vous utilisez Apache avec des drapeaux tels que -DSSL, il est nécessaire d'utiliser les mêmes drapeaux lors du test, par exemple, de l'utilisation de `httpd2 -S -DSSL`.

46.4.1 Hôtes virtuels à base de nom

Avec les hôtes virtuels à base de nom, plusieurs sites Web sont servis par adresse IP. Apache utilise le champ de l'hôte dans l'en-tête HTTP envoyé par le client pour connecter la requête à une entrée `ServerName` correspondante dans l'une des déclarations de l'hôte virtuel. Si aucun `ServerName` correspondant n'est trouvé, le premier `VirtualHost` spécifié est utilisé par défaut.

NameVirtualHost démarre la section Virtual Host dans une configuration Apache.

NameVirtualHost

NameVirtualHost indique au serveur Web Apache sur quelle adresse IP et, le cas échéant, sur quel port écouter les requêtes des clients contenant le nom de domaine dans l'en-tête HTTP.

Le premier argument peut être un nom de domaine complet, mais il est recommandé d'utiliser l'adresse IP. Le second argument est le port et il est facultatif. Par défaut, le port 80 est utilisé et configuré via la directive Listen (Sélection du périphérique réseau (p. 747)).

Il est possible d'utiliser le joker * pour l'adresse IP et le numéro du port pour recevoir des requêtes sur toutes les interfaces. Les adresses IPv6 doivent être placées entre crochets.

Exemple 46.8 *Variations des entées VirtualHost à base de nom*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:164::]:80
```

<VirtualHost></VirtualHost> dans le contexte à base de nom

Les blocs <VirtualHost></VirtualHost> contiennent les informations qui s'appliquent à un domaine particulier. Lorsque Apache reçoit une requête d'un client pour un VirtualHost défini, il utilise les directives contenues dans cette section. Toute directive Apache autorisée dans le contexte VirtualHost est utilisable ici. La balise VirtualHost d'ouverture prend les arguments suivants dans une configuration d'hôte virtuel à base de nom :

- adresse IP (ou nom de domaine pleinement qualifié) préalablement déclaré avec la directive NameVirtualHost.

- Numéro de port facultatif préalablement déclaré avec la directive `NameVirtualHost`.

Le joker * est également autorisé comme substitut de l'adresse IP. Cette syntaxe n'est valable que combinée à l'utilisation de jokers dans `NameVirtualHost *`. Lorsque vous utilisez des adresses IPv6, elles doivent être placées entre crochets.

***Exemple 46.9** Directives VirtualHost à base de nom*

```
<VirtualHost 192.168.1.100:80>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.100:80>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin webmaster@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
    # 2002:c0a8:164:: is the IPv6 equivalent to 192.168.1.100
    ServerName www.example.org
    DocumentRoot /srv/www/htdocs/example.org
    ServerAdmin webmaster@example.org
    ErrorLog /var/log/apache2/www.example.org-error_log
    CustomLog /var/log/apache2/www.example.org-access_log common
</VirtualHost>
```

Dans cet exemple, les domaines www.example.com et www.example.net sont hébergés sur la machine ayant l'adresse IP `192.168.1.100`. Le premier `VirtualHost` est celui par défaut pour toutes les requêtes entrantes vers le serveur Web.

Les directives `ErrorLog` (décrites dans la section intitulée « `ErrorLog` *`fichier | "|commande"`* » (p. 759)) et `CustomLog` (voir `http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog`) n'ont pas besoin de contenir le nom de domaine. Vous pouvez utiliser ici le nom de votre choix.

46.4.2 Hôtes virtuels à base d'adresse IP

Cette autre configuration d'hôte virtuel nécessite la configuration de plusieurs adresses IP pour une machine. Une instance d'Apache héberge plusieurs domaines, chacun ayant une adresse IP différente.

IMPORTANT: Adresses IP et hôtes virtuels à base d'adresse IP

Le serveur physique doit avoir une adresse IP pour chaque hôte virtuel à base d'adresse IP. Si la machine n'a pas plusieurs cartes réseau, il est également possible d'utiliser des interfaces réseau virtuelles (alias IP).

Configuration d'alias IP

Pour qu'Apache héberge plusieurs adresses IP, la machine physique doit accepter les requêtes pour plusieurs IP. C'est ce que l'on nomme l'hébergement multi-IP. De plus, la gestion d'alias IP doit être activée dans le kernel. C'est le paramètre par défaut dans SUSE Linux.

Lorsque le kernel a été configuré pour la gestion d'alias IP, les commandes `ifconfig` et `route` peuvent être utilisées pour définir des IP supplémentaires sur l'hôte. Ces commandes doivent être exécutées par un utilisateur `root`.

Pour l'exemple suivant, on suppose que l'hôte a déjà l'adresse IP `192.168.0.10` attribuée au périphérique réseau `eth0`. Entrez la commande `ifconfig` pour afficher l'adresse IP de l'hôte. Il est possible d'ajouter d'autres adresses IP avec les commandes suivantes :

```
ip addr add 192.168.0.20/24 dev eth0
ip addr add 192.168.0.30/24 dev eth0
```

Toutes ces adresses IP sont attribuées au même périphérique réseau physique (`eth0`).

`<VirtualHost></VirtualHost>` dans le contexte à base d'adresse IP

Une fois que la gestion d'alias IP a été configuré sur le système (ou que l'hôte a été équipé de plusieurs cartes réseau), Apache peut être configuré. Un bloc `VirtualHost` séparé est nécessaire pour chaque serveur virtuel.

L'exemple suivant montre Apache exécuté sur une machine ayant l'adresse IP `192.168.1.10`, hébergeant deux domaines sur les adresses IP supplémentaires `192.168.0.20` et `192.168.0.30`. Cet exemple particulier ne fonctionne que sur un réseau privé. En effet, les adresses IP de `192.168.0.0` à `192.168.0.255` ne sont pas routées vers Internet.

Exemple 46.10 *Directives VirtualHost à base d'adresse IP*

```
<VirtualHost 192.168.0.20>
   ServerName www.example.com
   DocumentRoot /srv/www/htdocs/example.com
   ServerAdmin webmaster@example.com
   ErrorLog /var/log/apache2/www.example.com-error_log
   CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.0.30>
   ServerName www.example.net
   DocumentRoot /srv/www/htdocs/example.net
   ServerAdmin tux@example.net
   ErrorLog /var/log/apache2/www.example.net-error_log
   CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>
```

Les directives `VirtualHost` ne sont ici spécifiées que pour les interfaces différentes de `192.168.0.10`. Lorsqu'une directive `Listen` (décrite dans Sélection du périphérique réseau (p. 747)) est également configurée pour `192.168.0.10`, un hôte virtuel à base d'adresse IP séparé doit être créé pour répondre aux requêtes HTTP vers cette interface. Sinon, les directives de la section `Main Server` de `/etc/apache2/httpd.conf` (voir la section intitulée « Directives Apache dans /etc/apache2/httpd.conf: Serveur principal » (p. 757)) sont appliquées.

46.5 Modules Apache

Le logiciel Apache a été conçu de façon modulaire : toutes les fonctionnalités excepté certaines tâches principales sont gérées par des modules. Ceci s'est tellement développé que même HTTP est traité par un module (http_core).

Les modules d'Apache peuvent être compilés dans le fichier binaire d'Apache lors de la génération ou chargés de façon dynamique lors de l'exécution. Pour le chargement lors de l'exécution, consultez la section intitulée « `LoadModule`

identificateur_module /chemin/vers/module » (p. 756) pour le chargement manuel des modules et Modules (p. 748) pour l'utilisation de YaST.

Apache dans SUSE Linux est accompagné des modules suivants, disponibles dans le RPM apache2 (préfixe "mod_" omis ici) : access, actions, alias, asis, auth, auth_anon, auth_dbm, auth_digest, auth_ldap, autoindex, cache, case_filter, case_filter_in, cern_meta, cgi, charset_lite, dav, dav_fs, deflate, dir, disk_cache, dumpio, echo, env, expires, ext_filter, file_cache, headers, imap, include, info, ldap, log_config, log_forensic, logio, mem_cache, mime, mime_magic, negotiation, proxy, proxy_connect, proxy_ftp, proxy_http, rewrite, setenvif, speling, ssl, status, suexec, unique_id, userdir, usertrack et vhost_alias. En outre, SUSE Linux offre les modules Apache suivants sous forme de paquetages RPM devant être installés séparément : apache2-mod_auth_mysql, apache2-mod_fastcgi, apache2-mod_macro, apache2-mod_murka, apache2-mod_perl, apache2-mod_php4, apache2-mod_php5, apache2-mod_python et apache2-mod_ruby.

Certains de ces modules sont documentés plus en détails dans cette section. Pour obtenir la description des autres modules dans la distribution de base, consultez le site Web des modules d'Apache à l'adresse http://httpd.apache.org/docs-2.0/mod/. Pour les modules tiers, consultez http://modules.apache.org/.

Les modules d'Apache se répartissent en trois catégories différentes : les modules de base, les modules d'extension et les modules externes.

46.5.1 Modules de base

Les modules de base sont compilés dans Apache par défaut. Ils sont disponibles, sauf s'ils sont explicitement ignorés lors de la génération. Dans Apache pour SUSE Linux, ne sont compilés que les modules de base minimum, mais ils sont tous disponibles en tant qu'*objets partagés* : plutôt que d'être inclus dans le fichier binaire /usr/sbin/httpd2 lui-même, ils peuvent être inclus lors de l'exécution en configurant APACHE_MODULES dans /etc/sysconfig/apache2.

Inclusions côté serveur avec mod_include

mod_include offre une méthode de traitement des fichiers avant l'envoi de données au client. Généralement, mod_include est utilisé pour inclure des fichiers dans un

document, qui sont à leur tour analysés en tant que HTML avant d'atteindre le client. C'est pourquoi ceci est désigné par l'expression inclusions côté serveur (SSI).

Avec les SSI, des commandes spéciales sont exécutées côté serveur, déclenchées par des commentaires SGML formatés. Ces commandes SGML ont la syntaxe suivante :

```
<!--#element attribute=value -->
```

Pour obtenir la listes des valeurs *element* et *attribute*, consultez la documentation de mod_include à l'adresse http://httpd.apache.org/docs-2.0/mod/mod_include.html.

Pour utiliser mod_include dans SUSE Linux, ajoutez include à APACHE_MODULES dans /etc/sysconfig/apache2 ou utilisez YaST comme indiqué dans Modules (p. 748).

ASTUCE

Utilisez la directive XBitHack (http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack) pour indiquer à Apache d'analyser les fichiers avec l'octet execute défini pour les directives SSI.

Cela signifie que plutôt que de devoir changer l'extension d'un fichier pour indiquer qu'il contient des éléments SSI (.shtml dans l'exemple ci-dessus), vous pouvez utiliser un fichier .html classique et exécuter chmod +x *myfile*.html.

Common Gateway Interface : mod_cgi

mod_cgi permet à Apache de fournir le contenu créé par des programmes ou des scripts CGI ("Common Gateway Interface") externes. Il agit en tant qu'instance entre un langage de programmation disponible sur la machine physique et le serveur Web Apache. En théorie, les scripts CGI peuvent être écrits dans n'importe quel langage de programmation. On utilise généralement des langages de type Perl ou C. mod_cgi est la méthode la plus courante pour inclure du contenu dynamique à un site Web.

La programmation CGI est différente de la programmation "classique" en ce que les programmes et les scripts CGI doivent pouvoir générer un type MIME `Content-type: text/html` pour produire un résultat HTML.

Exemple 46.11 *Un script CGI simple dans Perl*

```
#!/path/to/perl
print "Content-type: text/html\n\n";
print "Hello, World.";
```

La différence entre les modules spécifiquement liés à un langage de programmation (tels que `mod_php5`) et `mod_cgi` tient à la possibilité de combiner `mod_cgi` avec `mod_suexec` (voir la section intitulée « Exécution de CGI en tant qu'utilisateur différent avec `mod_suexec` » (p. 771)). Cette combinaison permet l'exécution des scripts CGI avec un ID d'utilisateur spécifié. Généralement, les scripts utilisant uniquement `mod_cgi` ou `mod_php5` sont exécutés avec l'ID d'utilisateur de l'utilisateur Apache (par défaut dans SUSE Linux: `wwwrun`). Les modules conçus pour un langage de programmation (tels que `mod_php5` ou `mod_ruby`) incorporent un interpréteur persistant dans Apache pour exécuter les scripts sous l'ID d'utilisateur d'Apache.

En conséquence, les CGI avec `mod_suexec` contribuent à la clarté d'administration car les processus CGI peuvent être affectés à des utilisateurs individuels plutôt qu'au serveur Web lui-même. En outre, cette combinaison contribue à une meilleure sécurité du système de fichiers : le script hérite uniquement des droits du système de fichiers de l'utilisateur. Dans le cas contraire des modules, le script se voit accorder les autorisations d'accès au fichier de l'utilisateur du serveur Web, ce qui peut se traduire par une visibilité involontaire des données du système de fichiers.

Les CGI se terminent à la fin de la requête d'un client sur le serveur Web. Cela signifie que les CGI ne sont pas persistants et libèrent toutes les ressources occupées à la fin. Ceci est un avantage, en particulier dans le cas d'une programmation erronée. Avec les modules, les effets des erreurs de programmation peuvent s'accumuler, du fait que l'interpréteur est persistant. Ceci peut conduire à l'impossibilité de libérer les ressources, telles que les connexions à la base de données, et nécessiter le rédemarrage d'Apache.

Pour utiliser `mod_cgi` dans SUSE Linux, ajoutez `cgi` à `APACHE_MODULES` dans `/etc/sysconfig/apache2` ou utilisez YaST comme indiqué dans Modules (p. 748). Le répertoire par défaut des CGIs dans SUSE Linux est `/srv/www/cgi-bin/`.

Si vous modifiez manuellement le fichier de configuration d'Apache, utilisez cet exemple comme guide pour configurer `mod_cgi`.

Exemple 46.12 *Activation manuelle de mod_cgi*

```
# Global Environment
LoadModule cgi_module /path/to/mod_cgi.so

# Main Server and/or Virtual Host and/or
# Directory and/or .htaccess context
AddHandler cgi-script .cgi .pl

# Main Server and/or Virtual Host context
ScriptAlias /cgi-bin/ /srv/www/cgi-bin/

# Alternatively, explicitly allow CGI scripts in a directory
# Main Server and/or Virtual Host context
<Directory /srv/www/some/dir>
   Options +ExecCGI
<Directory>
```

46.5.2 Modules d'extension

En général, les modules libellés comme des extensions sont inclus dans le paquetage logiciel d'Apache, mais ne sont généralement pas compilés dans le serveur de façon statique. Dans SUSE Linux, ils sont disponibles en tant qu'objets partagés pouvant être chargés dans Apache lors de l'exécution.

Exécution de CGI en tant qu'utilisateur différent avec `mod_suexec`

Combiné à `mod_cgi` (la section intitulée « Common Gateway Interface : `mod_cgi` » (p. 769)), `mod_suexec` permet l'exécution des scripts CGI en tant qu'utilisateur ou que groupe spécifique. Le programme suEXEC de `/usr/sbin/suexec2` est utilisé à cette fin. Il s'agit d'un wrapper appelé par Apache chaque fois qu'un script ou un programme CGI est exécuté. Le wrapper et le programme se voient ensuite affecter l'ID de l'utilisateur et du groupe configuré. L'exécution s'effectue de ce fait en tant que l'utilisateur ou le groupe configuré.

Bien que cette approche réduise de façon considérable les risques de sécurité liés à la génération de scripts CGI par l'utilisateur, elle n'est pas sans susciter des préoccupations importantes :

Considérations liées à l'utilisation de suEXEC

- `suEXEC docroot`—Toute exécution de script est limitée à ce répertoire de base. Cela signifie que l'exécution de scripts avec suexec en dehors de `docroot` est impossible et se traduit par une erreur. `docroot` est défini lors de la compilation de `suEXEC` et ne peut être modifié lors de l'exécution. Le répertoire par défaut dans SUSE Linux est `/srv/www`.

- `uidmin`—Ceci représente l'ID minimum que doit posséder un utilisateur pour exécuter des scripts avec `suEXEC`. Ceci évite l'exécution de scripts par des utilisateurs système tels que `root`. Ne créez pas d'utilisateurs dont l'ID soit inférieur à `uidmin` s'il doit être utilisé avec `mod_suexec`. L'`uidmin` par défaut dans SUSE Linux est 96.

- `gidmin`—C'est le même concept que `uidmin`, mais pour l'ID du groupe. le `gidmin` par défaut dans SUSE Linux est 96.

- Autorisations d'accès aux répertoires et aux fichiers—Le script en question doit être détenu par le même utilisateur et appartenir au groupe tel que spécifié dans l'utilisateur et le groupe de `suEXEC`. De surcroît, le fichier ne doit pas pouvoir être écrit par quiconque excepté son propriétaire. De la même manière, le répertoire dans lequel réside le script ne doit pas pouvoir être écrit par quiconque excepté son propriétaire.

- `suEXEC safepath`—Tous les programmes utilisés dans un script (tel que Perl) doivent résider dans les chemins désignés comme sécurisés pour suexec. `safepath` est défini lors de la compilation de `suEXEC` et ne peut être modifié lors de l'exécution. Le chemin `safepath` par défaut dans SUSE Linux est `/usr/local/bin:/usr/bin:/bin`.

En cas d'erreurs provoquées par `mod_suexec`, consultez le fichier journal de suexec dans `/var/log/apache2/suexec.log`.

Pour utiliser `mod_suexec` dans SUSE Linux, ajoutez `suexec` à `APACHE_MODULES` dans `/etc/sysconfig/apache2` ou utilisez YaST comme indiqué dans Modules (p. 748). N'oubliez pas que `mod_cgi` est nécessaire pour exécuter suexec.

mod_suexec est très utile lorsqu'il est appliqué dans un environnement d'hôte virtuel, décrit dans Section 46.4, « Hôtes virtuels » (p. 763). Pour spécifier un certain utilisateur et un certain groupe exécutant des scripts CGI, utilisez la syntaxe suivante dans le fichier contenant les déclarations de l'hôte virtuel (par défaut dans SUSE : /etc/apache2/vhosts.d/*) :

Exemple 46.13 *Configuration de mod_suexec*

```
<VirtualHost 192.168.0>
# ...
ScriptAlias /cgi-bin/ /srv/www/vhosts/www.example.com/cgi-bin/
SuexecUserGroup tux users
# ...
</VirtualHost>
```

La syntaxe SuexecUserGroup *nom d'utilisateur groupe* de cet exemple affecte à tous les scripts résidant dans /srv/www/vhosts/www.example.com/cgi-bin/ l'ID d'utilisateur tux et l'ID de groupe des utilisateurs.

Secure Sockets Layer et Apache : mod_ssl

mod_ssl fournit le cryptage renforcé et utilise les protocoles secure sockets layer (SSL) et transport layer security (TLS) pour la communication HTTP entre un client et le serveur Web. À cette fin, le serveur envoie un certificat SSL contenant des informations prouvant l'identité valide du serveur avant la réponse à toute requête vers une adresse URL. Ceci garantit à son tour que le serveur est le seul point terminal correct pour la communication. De plus, le certificat génère une connexion codée entre client et serveur, capable de transporter des informations sans risque d'exposer du contenu sensible en texte brut. L'effet le plus visible de l'utilisation de mod_ssl avec Apache est que les adresses URL portent le préfixe https:// et non http://.

Le port par défaut pour les requêtes SSL et TLS du côté du serveur Web est 443. Il n'y a pas de conflit entre une écoute « normale » Apache sur le port 80 et une écoute Apache de type SSL/TLS sur le port 443. En fait, HTTP et HTTPS peuvent être exécutés avec la même instance Apache. Un hôte virtuel (voir Section 46.4, « Hôtes virtuels » (p. 763)) est généralement utilisé pour envoyer les requêtes vers le port 80 et le port 443 afin de séparer les serveurs virtuels.

IMPORTANT: Hôtes virtuels à base de nom et SSL

Il n'est pas possible d'exécuter plusieurs hôtes virtuels de type SSL sur un serveur avec une seule adresse IP. Les utilisateurs qui se connectent à ce type de configuration reçoivent un message d'avertissement indiquant que le certificat ne correspond pas au nom du serveur chaque fois qu'ils visitent l'adresse URL. Une adresse IP ou un port séparés sont nécessaires pour chaque domaine SSL afin de réaliser la communication basée sur un certificat SSL valide.

Malgré le message d'avertissement, vous obtenez le même niveau de codage que sur n'importe quel site SSL valide. Cela signifie que tant que le message d'avertissement est acceptable, la communication entre le serveur Web et le client est sécurisée. Le concept de la connaissance de l'identité unique du serveur, garantie par un certificat SSL valide, est abandonné.

Pour activer `mod_ssl` dans SUSE Linux, ajoutez `ssl` à `APACHE_MODULES` dans `/etc/sysconfig/apache2` ou utilisez YaST comme indiqué dans Modules (p. 748). En outre, le serveur Web doit être configuré pour écouter le port HTTPS standard 443. Ceci peut s'effectuer manuellement dans `/etc/apache2/listen.conf` ou dans YaST via l'entrée du menu *Écoute* (voir Sélection du périphérique réseau (p. 747)).

Il est possible de créer un certificat SSL de test en saisissant `cd /usr/share/doc/packages/apache2; ./certificate.sh` en tant que `root`. Suivez les instructions à l'écran pour générer le certificat SSL. Les fichiers de certificat résultants résident dans les répertoires `/etc/apache2/ssl*`.

Un certificat « réel » avec une validité globale peut être obtenu auprès de fournisseurs tels que Thawte (`http://www.thawte.com/`) ou Verisign (`www.verisign.com`).

Si vous modifiez manuellement le fichier de configuration d'Apache, utilisez cet exemple comme guide pour configurer `mod_ssl`.

Exemple 46.14 *Configuration manuelle de mod_ssl*

```
# Global Environment
# listen on the standard SSL port
Listen 443
# load module only if rcapache2 start-ssl was issued
<IfDefine SSL>
LoadModule ssl_module /path/to/mod_ssl.so
</IfDefine>

# Main Server context
# include global (server-wide) SSL configuration
# that is not specific to any virtual host
# only if ssl_module was loaded
<IfModule mod_ssl.c>
Include /etc/apache2/ssl-global.conf
</IfModule>
```

ASTUCE

N'oubliez pas d'ouvrir le pare-feu pour Apache avec SSL sur le port 443. Ceci peut s'effectuer via YaST, dans *Sécurté et Utilisateurs* → *Pare-feu* → *Services autorisés*. Ajoutez ensuite *Serveur HTTPS* à la liste des *Services autorisés*.

46.5.3 Modules externes

Officiellement, les modules baptisés externes ne sont pas inclus dans la distribution d'Apache. Néanmoins, SUSE Linux en fournit plusieurs qui sont prêts à l'usage. Ce chapitre explique brièvement certains modules externes et leur fonctionnalité.

Utilisation de Perl pour gérer Apache : `mod_perl`

`mod_perl` incorpore un interpréteur Perl persistant dans Apache. Ceci évite la surcharge causée par un `mod_cgi` qui appelle un exécutable externe sur chaque requête vers un CGI. `mod_perl` permet en outre le contrôle de nombreux aspects des fonctionnalités Apache avec l'aide du langage de programmation Perl.

Pour utiliser `mod_perl` dans SUSE Linux, installez le RPM `apache2-mod_perl` et activez le module soit via YaST (Modules (p. 748)) soit manuellement dans `/etc/sysconfig/apache2`. Après installation et activation, un fichier de configuration séparé, `mod_perl.conf`, est placé dans `/etc/apache2/conf.d/`. De surcroît, le script de démarrage `mod_perl` est installé en tant que `mod_perl-startup.pl`.

Pour plus d'informations sur l'utilisation du module, consultez la documentation qui se trouve sur le site Web mod_perl (http://perl.apache.org/).

Service de PHP : mod_php4, mod_php5

PHP est un langage de programmation courant, destiné à l'origine à être utilisé sur le Web. Il existe en deux versions, PHP4 et PHP5. Alors que PHP4 représente le concept et l'approche classiques de PHP, PHP5 a introduit de nouvelles possibilités de programmation orientées objet ainsi que de nombreuses autres fonctions avancées. mod_php4 et mod_php5 sont disponibles dans SUSE Linux. Ils incorporent l'interpréteur PHP dans Apache en tant que module persistant.

Pour utiliser mod_php4 ou mod_php5 dans SUSE Linux, installez le RPM correspondant (apache2-mod_php4, apache2-mod_php5) et activez le module soit via YaST (Modules (p. 748)) soit manuellement dans /etc/sysconfig/apache2.

Après installation et activation, un fichier de configuration séparé correspondant au module, (php4.conf ou php5.conf), est placé dans /etc/apache2/conf.d/. Le site Web PHP (http://www.php.net) est une excellente ressource pour utiliser Apache avec PHP.

Python et Apache : mod_python

mod_python incorpore l'interpréteur Python dans Apache. Python est un langage de programmation orienté objet avec une syntaxe très claire et lisible. Une fonction inhabituelle mais pratique est que la structure du programme dépend de la mise en retrait du code source plutôt que d'éléments de démarcation classiques tels que begin et end.

Pour utiliser mod_python dans SUSE Linux, installez le RPM apache2-mod_python et activez le module soit via YaST (Modules (p. 748)) soit manuellement dans /etc/sysconfig/apache2. Pour plus d'informations sur l'utilisation du module, consultez la documentation qui se trouve sur le site Web mod_python (http://www.modpython.org/).

Interpréteur Ruby dans Apache : mod_ruby

mod_ruby incorpore l'interpréteur Ruby dans le serveur Web Apache, pour permettre l'exécution des scripts Ruby CGI en mode natif. Ruby est un langage de programmation

orienté objet de haut niveau relativement nouveau qui ressemble à certains aspects de Perl et de Python. Tout comme Python, il a une syntaxe claire et transparente. Par contre, Ruby a adopté des abréviations (telles que `$.r` pour le numéro de la dernière ligne lue dans le fichier d'entrée) qui sont appréciées de certains programmeurs et que d'autres n'aiment pas. Le concept de base de Ruby ressemble étroitement à celui de Smalltalk.

Pour utiliser `mod_ruby` dans SUSE Linux, installez le RPM `apache2-mod_ruby` et activez le module soit via YaST (Modules (p. 748)) soit manuellement dans `/etc/sysconfig/apache2`. Pour plus d'informations sur l'utilisation du module, consultez la documentation qui se trouve sur le site Web mod_ruby (`http://www.modruby.net/en/index.rbx`).

Accès au système de fichiers natif : `mod_dav`

`mod_dav` fournit la fonctionnalité WebDAV (création et gestion de versions distribuées sur le Web) d'Apache. WebDAV est une extension du protocole HTTP qui permet aux utilisateurs de modifier et de gérer des fichiers de façon collaborative sur des serveurs distants. Les fonctionnalités de WebDAV sont similaires à celles de FTP à la différence majeure que HTTP est utilisé comme protocole sous-jacent pour l'accès au serveur. En effet, `mod_dav` fait d'un serveur Web Apache un système de fichiers distant avancé.

Il est recommandé, sinon nécessaire, de limiter l'accès aux répertoires disponibles via WebDAV. Les précautions minimales consistent à configurer l'authentification HTTP de base pour la ressource WebDAV, ainsi que les clauses Limit à l'intérieur d'une directive `Emplacement`.

Pour accéder à une ressource WebDAV, un logiciel compatible WebDAV doit se trouver du côté du client. SUSE Linux est accompagné de fonctionnalités WebDAV : `Konqueror` avec le préfixe `webdav://` ou `webdavs://` (pour WebDAV sur des connexions SSL) permet de se connecter à un système de fichiers Apache WebDAV.

`mod_dav` nécessite le module `mod_dav_fs`, qui fournit l'accès au système de fichiers pour WebDAV. Pour utiliser `mod_dav` dans SUSE Linux, activez le module soit via YaST (Modules (p. 748)) soit manuellement dans `/etc/sysconfig/apache2`. Faites de même pour `mod_dav_fs`. Pour plus d'informations sur l'utilisation du module, consultez la documentation qui se trouve sur le site Web mod_dav (`http://httpd.apache.org/docs-2.0/mod/mod_dav.html`).

Offre de pages d'accueil utilisateurs : mod_userdir

Par défaut, mod_userdir dans SUSE Linux offre le contenu du dossier ~/public_html de chaque utilisateur comme des pages Web publiques. L'URL permettant d'accéder à ces pages est alors http://www.example.com/~*nom d'utilisateur*/.

ASTUCE

mod_userdir dans SUSE Linux interdit l'accès à tous les répertoires du répertoire d'accueil de l'utilisateur root pour des raisons de sécurité. Vous pouvez en outre autoriser spécifiquement certains utilisateurs à posséder des pages d'accueil publiques en utilisant :

```
# Main server context
UserDir disabled
UserDir enabled tux wilber
```

Pour utiliser mod_userdir dans SUSE Linux, activez le module soit via YaST (Modules (p. 748)) soit manuellement dans /etc/sysconfig/apache2. Pour plus d'informations sur l'utilisation du module, consultez la documentation qui se trouve sur le site Web mod_userdir (http://httpd.apache.org/docs-2.0/mod/mod_userdir.html).

Modification de la configuration de l'adresse URL : mod_rewrite

mod_rewrite est souvent nommé « le couteau de l'armée suisse pour la manipulation des adresses URL. » Il réécrit les adresses URL demandées à la volée selon un ensemble de règles spécifié. Le résultat ressemble généralement à http://www.example.com/2/1/de pour http://www.example.com/display.php?cat=2&article=1&lang=de.

Le Guide de réécriture d'adresse URL explique les avantages et les inconvénients de ce module puissant mais complexe :

« Avec mod_rewrite, soit vous vous suicidez dès la première fois, soit vous en tombez amoureux pour le restant de vos jours du fait de sa puissance. »

Des ensembles RewriteRule peuvent être définis dans tous les contextes de configuration : pour le serveur principal, pour les hôtes virtuels, pour les répertoires et pour les fichiers .htaccess. Un bon point de départ pour la réécriture d'adresses URL avec mod_rewrite est le Guide de réécriture d'adresse URL à l'adresse http://httpd.apache.org/docs-2.0/misc/rewriteguide.html.

Pour utiliser mod_rewrite dans SUSE Linux, activez le module soit via YaST (Modules (p. 748)) soit manuellement dans /etc/sysconfig/apache2.

46.6 Sécurité

Un serveur Web exposé à Internet nécessite des efforts d'administration incessants. Il est inévitable que des problèmes de sécurité surviennent, qu'ils soient liés aux logiciels ou à une erreur de configuration. Voici quelques conseils qui vous permettront de les gérer.

Mises à jour

Si des failles sont détectées dans le logiciel Apache, un avertissement de sécurité est diffusé par SUSE. Il contient des instructions permettant de corriger les failles, qui doivent être appliquées dès que possible. La liste de diffusion des annonces de sécurité de SUSE se trouve à l'adresse http://www.suse.com/us/private/support/online_help/mailinglists/. Les informations les plus récentes concernant les problèmes de sécurité des paquetages SUSE Linux sont également disponibles en ligne à l'adresse http://www.novell.com/linux/security/securitysupport.html.

En outre, nous vous conseillons de vous abonner à la liste de diffusion des annonces d'Apache (http://httpd.apache.org/lists.html#http-announce), dans laquelle des versions et des correctifs sont publiés.

Autorisations DocumentRoot

Par défaut dans SUSE Linux, le répertoire DocumentRoot /srv/www/htdocs et le répertoire CGI /srv/www/cgi-bin appartiennent à l'utilisateur root. Vous ne devez pas changer ces autorisations. Si tout le monde pouvait écrire dans les cépertoires, n'importe quel utilisateur pourrait y placer des fichiers. Ces fichiers pourraient ensuite être exécutés par Apache avec les autorisations wwwrun, qui peuvent donner à l'utilisateur un accès involontaire aux ressources du système de fichiers. Utilisez les sous-répertoires /srv/www/htdocs et /srv/www/

cgi-bin pour organiser les données d'un utilisateur ou d'un domaine en combinaison avec la directive Directory (voir Répertoire (p. 750)).

Répertoires CGI et SSI

Les scripts interactifs en Perl, PHP, SSI ou n'importe quel autre langage de programmation peuvent surtout exécuter des commandes arbitraires. La limitation de l'exécution de CGI et de SSI (voir la section intitulée « Common Gateway Interface : mod_cgi » (p. 769), ScriptAlias (p. 751) et la section intitulée « Inclusions côté serveur avec mod_include » (p. 768)) à des répertoires spécifiques au lieu de les autoriser de façon globale est une option qui permet de réduire les risques.

Une autre possibilité consiste à utiliser mod_suexec (voir la section intitulée « Exécution de CGI en tant qu'utilisateur différent avec mod_suexec » (p. 771)) pour les CGI en général. Pour les modules Apache, une configuration tenant compte de la sécurité pour les interpréteurs, comme dans la section intitulée « Service de PHP : mod_php4, mod_php5 » (p. 776), contribue à la conservation d'un environnement Web sécurisé.

Autorisations d'accès

Il est fréquent, en particulier dans les environnements de test, que les autorisations d'accès à un serveur Web soient gérées avec désinvolture du fait de la nature de test d'une configuration. Ceci peut se traduire par le dévoilement accidentel d'informations sensibles, voire par l'exposition d'un serveur entier à un public qui ne devrait pas y accéder. Utilisez la directive Order (http://httpd.apache.org/docs-2.0/mod/mod_access.html#order) en combinaison avec des fichiers .htaccess (voir la section intitulée « *noms de fichier* AccessFileName » (p. 759)) pour restreindre l'accès à certains sites Web à des utilisateurs ou à des clients spécifiques.

Vous pouvez également utiliser l'approche « sécurité par obscurcissement ». Un exemple classique consiste à exécuter Apache sur un port non standard (voir Sélection du périphérique réseau (p. 747)). Ceci se traduit par l'ajout du port aux URL, par exemple http://www.example.com:8765, ce qui est acceptable dans des environnements de test.

46.7 Dépannage

Si Apache ne démarre pas, si la page Web n'est pas accessible ou si les utilisateurs ne peuvent pas se connecter au serveur Web, il est important de déterminer la cause du problème. Voici quelques endroits classiques à consulter pour trouver des explications aux erreurs et pour vérifier des points importants.

Tout d'abord, `rcapache2` (décrit dans Section 46.3.3, « Activation, démarrage et arrêt d'Apache » (p. 761)) est détaillé concernant les erreurs et peut être très utile s'il est utilisé avec Apache. Il est parfois tentant d'utiliser le binaire `/usr/sbin/httpd2` pour démarrer ou arrêter le serveur Web. Evitez de le faire et utiliser plutôt le script `rcapache2`. `rcapache2` fournit même des conseils et des astuces pour résoudre des erreurs de configuration.

En second lieu, on ne soulignera jamais assez l'importance des fichiers journaux (voir la section intitulée « Fichiers journaux » (p. 745)). En cas d'erreur irrécupérable ou non fatale, les fichiers journaux d'Apache permettent d'en rechercher les causes. En outre, vous pouvez contrôler le niveau de commentaires des messages consignés grâce à la directive `LogLevel` (voir la section intitulée « *niveau* `LogLevel` » (p. 760)) si vous avez besoin de davantage de détails dans les fichiers journaux.

ASTUCE

Consultez les messages des journaux d'Apache à l'aide de la commande `tail -F /var/log/apache2/*_log &`. Exécutez ensuite `rcapache2 restart`. Tentez à présent de vous connecter à un navigateur et vérifiez le résultat.

Une erreur courante consiste à ne pas ouvrir les ports Apache dans la configuration du pare-feu du serveur. Si vous configurez Apache avec YaST, une option séparée permet de gérer ce problème spécifique.

Si l'erreur ne peut être retrouvée par ces moyens, consultez la base de données en ligne des bogues Apache à l'adresse `http://httpd.apache.org/bug_report.html`. De surcroît, vous pouvez communiquer avec la communauté des utilisateurs d'Apache via une liste de diffusion qui se trouve à l'adresse `http://httpd.apache.org/userslist.html`. Vous trouverez un groupe de discussion recommandé à l'adresse `comp.infosystems.www.servers.unix`.

46.8 Pour plus d'informations

Apache est un serveur Web largement utilisé. En conséquence, de nombreux sites Web offrent une assistance et de l'aide, avec des niveaux de qualité variables. Dans tous les cas, le point de départ de toute recherche concernant Apache et ses possibilités reste http://httpd.apache.org/docs-2.0/.

De plus, le paquetage RPM apache2-doc contient le manuel d'Apache pour l'installation locale et les références. Pour trouver certaines astuces de configuration spécifiques de SUSE, le fichier /usr/share/doc/packages/apache2 contient un aide-mémoire.

Le paquetage RPM apache2-example-pages contient quelques exemples de pages d'Apache montrant des informations concernant le serveur Web.

46.8.1 Modules Apache

Vous trouverez des informations complémentaires sur les modules externes d'Apache de Section 46.5.3, « Modules externes » (p. 775) en consultant :

- httpd.apache.org/docs-2.0/mod/
- http://www.php.net/manual/en/install.unix.apache2.php
- http://www.modpython.org/
- http://www.modruby.net/
- http://perl.apache.org/

46.8.2 CGI

Des informations complémentaires sur l'utilisation de mod_cgi (voir la section intitulée « Common Gateway Interface : mod_cgi » (p. 769)) et sur la programmation de CGI sont disponibles ci-dessous :

- http://www.modperl.com/

- http://www.modperlcookbook.org/
- http://www.fastcgi.com/
- http://www.boutell.com/cgic/

46.8.3 Sources diverses

Si vous éprouvez des difficultés spécifiques avec Apache dans SUSE Linux, consultez la base de données de support SUSE à l'adresse http://portal.suse.com/sdb/en/index.html.

Vous pouvez consulter l'historique d'Apache à l'adresse http://httpd.apache.org/ABOUT_APACHE.html. Cette page explique également pourquoi le serveur a été baptisé Apache.

Des informations concernant la mise à niveau de la version 1.3 vers la version 2.0 sont disponibles à l'adresse http://httpd.apache.org/docs-2.0/en/upgrading.html.

47 Synchronisation des fichiers

De nos jours, nombreux sont ceux qui utilisent plusieurs ordinateurs : un ordinateur à la maison, un ou plusieurs ordinateurs sur le lieu de travail et éventuellement en plus un ordinateur portable ou un assistant personnel pour les déplacements. On a besoin d'une grande quantité de fichiers sur tous ces ordinateurs et il est important de pouvoir travailler avec n'importe quel ordinateur, modifier ces fichiers et disposer de leur version la plus récente sur tous les ordinateurs.

47.1 Logiciels pour la synchronisation des données

Sur des ordinateurs reliés en permanence entre eux par un réseau rapide, la synchronisation de fichiers ne pose aucun problème. Dans ce cas, ill suffit de choisir un système de fichiers réseau, comme NFS et d'enregistrer les fichiers sur un serveur. Ensuite, tous les ordinateurs accèdent aux mêmes données par l'intermédiaire du réseau. Cette méthode ne fonctionne pas dans le cas d'une mauvaise connexion réseau ou si la liaison n'est pas permanente. Les personnes qui voyagent avec un ordinateur portable sont amenées à avoir des copies de tous les fichiers sur le disque dur local. Mais lorsque les fichiers sont modifiés, le problème de la synchronisation se pose vite. Si un fichier a été modifié sur un ordinateur, il faut veiller à actualiser aussi la copie du fichier sur tous les autres ordinateurs. Si cette situation ne se produit que de temps en temps, les procédures de copie manuelle à l'aide de scp ou de rsync sont suffisantes. Avec une plus grande quantité de données, la tâche se complique rapidement et requiert une grande attention de la part de l'utilisateur pour éviter des erreurs, comme le remplacement d'une nouvelle version d'un fichier par une version plus ancienne.

AVERTISSEMENT: Risque de perte de données

Il faut de toute façon se familiariser avec le logiciel utilisé et tester ses fonctions avant de gérer ses données à l'aide d'un système de synchronisation. Pour les données importantes, une sauvegarde est indispensable.

Pour s'épargner le travail fastidieux de la synchronisation manuelle des données comportant, en outre, un risque élevé d'erreurs, il existe des logiciels qui automatisent cette tâche en se basant sur différentes méthodes. Les brefs aperçus suivants ont pour but de donner à l'utilisateur une idée de fonctionnement et de l'utilisation de ces logiciels. Avant de les mettre en œuvre réellement, il vaut mieux lire attentivement la documentation y afférant.

47.1.1 Unison

Dans le cas d'Unison, il ne s'agit pas d'un système de fichiers réseau. Ici, en revanche, on enregistre les fichiers et on travaille avec ces derniers tout à fait normalement en local. Le programme Unison peut être appelé manuellement pour synchroniser des fichiers. Lors de la première synchronisation, une base de données est créée sur les deux ordinateurs concernés, dans laquelle sont enregistrés les sommes de contrôle, les pointeurs temporels et les autorisations des fichiers sélectionnés. Lors de l'appel suivant, unison peut reconnaître quels fichiers ont été modifiés et en proposer la transmission d'un ordinateur vers l'autre. En règle générale, on peut accepter toutes les propositions.

47.1.2 CVS

Utilisé en général pour la gestion de versions de textes sources de logiciels, CVS offre la possibilité de disposer des copies de fichiers sur plusieurs ordinateurs. Il se prête donc parfaitement à ce que nous recherchons. Dans le cas de CVS, il existe une base de données centrale (repository, ou en français, un référentiel) sur le serveur qui ne stocke pas seulement les fichiers mais également les modifications de ces fichiers. Toute modification effectuée localement est validée (commit) dans la base de données pour être reprise (update) par d'autres ordinateurs. Les deux procédures doivent être préparées par l'utilisateur.

En ce qui concerne les modifications, CVS est très tolérant vis-à-vis des erreurs : les modifications sont rassemblées, et il n'y a conflit que si des modifications ont été appor-

tées aux mêmes lignes. Dans ce cas, la base de données reste dans un état stable, le conflit est visible et doit être résolu sur l'ordinateur client.

47.1.3 subversion

Contrairement à CVS qui « a évolué », subversion est un projet développé de façon consistante ; subversion a été créé pour remplacer avantageusement CVS d'un point de vue technique.

Il est clair que subversion apporte une amélioration à CVS dans de nombreux domaines. En raison de son histoire, CVS ne gère que les fichiers et ignore tout des répertoires. Dans subversion, au contraire, les répertoires possèdent aussi un historique de versions et peuvent également être copiés et renommés exactement comme les fichiers. En outre, il est possible d'ajouter à chaque fichier et à chaque répertoire des métadonnées qui sont également soumises à la gestion des versions. À la différence de CVS, subversion offre un accès réseau transparent grâce à quelques protocoles comme WebDAV (Web-based Distributed Authoring and Versioning). WebDAV étend la fonctionnalité du protocole HTTP pour permettre l'accès en écriture en collaboration aux fichiers sur les serveurs Web distants.

La réalisation de subversion s'est en grandes parties basées sur des applications existantes. Pour cette raison, le serveur Web Apache et l'extension WebDAV sont toujours utilisés en conjonction avec subversion.

47.1.4 mailsync

Comparé aux outils de synchronisation mentionnés jusque-là, mailsync sert uniquement à la synchronisation des messages électroniques entre les différentes boîtes aux lettres. Il peut s'agir aussi bien des fichiers de boîtes aux lettres locaux que de ceux des boîtes aux lettres hébergées sur un serveur IMAP.

Il est décidé, en fonction de l'identificateur de message (message ID) contenu dans l'en-tête du message électronique, individuellement pour chaque message s'il doit être sychronisé ou effacé. Une synchronisation est possible autant entre les différentes boîtes aux lettres qu'entre les hiérarchies de boîtes aux lettres.

47.1.5 rsync

Lorsque vous n'avez pas besoin du contrôle de versions mais que vous souhaitez synchroniser de grandes arborescences de fichiers sur des connexions réseau lentes, l'outil rsync est fait pour vous. rsync dispose de mécanismes minutieux pour transférer exclusivement des modifications dans les fichiers. Cela ne concerne pas seulement les fichiers texte, mais également les fichiers binaires. Pour reconnaître les différences entre fichiers, rsync répartit les fichiers en blocs et calcule des sommes de contrôle correspondant à ces blocs.

L'effort consenti à reconnaître les modifications a aussi un prix. Pour que rsync fonctionne, il faut redimensionner généreusement les ordinateurs qui doivent être synchronisés. Il n'est surtout pas question d'économiser sur la mémoire vive (RAM).

47.2 Critères de choix du logiciel

47.2.1 Comparaison client-serveur et pair à pair

Deux modèles différents de distribution des données sont répandus. Dans le premier modèle, tous les ordinateurs (appelés clients) synchronisent leurs données avec un serveur central. Le serveur doit être accessible à tous les clients au moins de temps en temps. Ce modèle est utilisé par subversion, CVS et WebDAV.

Dans l'autre modèle, tous les ordinateurs connectés par le réseau peuvent synchroniser mutellement leurs données en tant que pairs. Cette méthode est utilisée par unison. rsync fonctionne en réalité en mode client, mais on peut utiliser chaque client en tant que serveur.

47.2.2 Portabilité

Subversion, CVS et unison sont également disponibles sur de nombreux autres systèmes d'exploitation comme les autres Unix et sous Windows.

47.2.3 Comparaison des modes Interactif et automatique

Dans le cas de subversion, de CVS, de WebDAV et de unison, la synchronisation de données est lancée manuellement par l'utilisateur. Ce comportement permet de contrôler plus précisément les données à synchroniser et de gérer plus aisément les conflits. En revanche, si la synchronisation est réalisée trop rarement, les risques de conflit sont augmentés.

47.2.4 Conflits : apparition et solutions

Dans le cas de subversion ou de CVS, il est rare qu'un conflit survienne, même si plusieurs personnes collaborent pour un même gros projet logiciel. Ceci est dû au fait que les documents sont vérifiés ligne par ligne. En cas de conflit, cela ne concerne toujours qu'un seul client. Un conflit est en principe facile à résoudre avec subversion ou CVS.

Dans le cas d'unison, vous êtes informé des conflits et il est possible d'éviter la synchronisation du fichier. En revanche, les modifications ne sont pas aussi faciles à effectuer qu'avec subversion ou CVS.

Alors que dans subversion ou CVS il est également possible d'enregistrer partiellement des modifications en cas de conflit, WebDAV ne procède à la validation que si l'ensemble de la modification réussit.

rsync n'offre aucun moyen de traiter les conflits. L'utilisateur doit veiller lui-même à ne pas écraser des fichiers par erreur et à résoudre à la main tous les conflits susceptibles d'apparaître. Pour ne pas courir de risques, on peut utiliser aussi un système de contrôle de versions comme RCS.

47.2.5 Sélectionner et ajouter des fichiers

Dans la configuration par défaut d'Unison, toute la structure arborescente du répertoire est synchronisée. Les nouveaux fichiers qui s'y présentent sont automatiquement concernés par la synchronisation.

Avec subversion ou CVS, les nouveaux répertoires et fichiers doivent être ajoutés explicitement au moyen de `svn add` et `cvs add` respectivement. Ceci permet un contrôle précis des fichiers à synchroniser. En revanche, de nouveaux fichiers sont souvent négligés, surtout si, à cause du nombre important de fichiers, les points d'interrogation affichés par `svn update` et `svn status` ou `cvs update` sont ignorés.

47.2.6 Historique

Subversion et CVS offrent une fonctionnalité supplémentaire qui permet la reconstitution des anciennes versions de fichiers. Lors de chaque modification, il est possible d'ajouter une brève note de travail, permettant de suivre ensuite facilement le développement des fichiers grâce au contenu et aux annotations. Ceci constitue une aide très utile pour les projets de fin d'études et les textes de logiciels.

47.2.7 Volume de données et espace disque dur

On a besoin sur tous les ordinateurs concernés de suffisamment d'espace libre sur le disque dur pour héberger toutes les données réparties. Dans le cas de subversion et de CVS, il faut en plus prévoir de l'espace sur le serveur pour la base de données du référentiel. L'historique des fichiers étant également enregistré sur le serveur, l'espace nécessaire est encore plus important. Pour les fichiers au format texte, la place occupée est relativement raisonnable car seules les lignes modifiées sont à nouveau enregistrées. En revanche, pour les fichiers binaires, l'encombrement augmente à chaque modification de la taille du fichier.

47.2.8 GUI, interface utilisateur graphique

Unison offre une interface utilisateur graphique qui affiche les procédures de synchronisation qu'Unison veut réaliser. Vous pouvez accepter la proposition ou rejeter certains fichiers de la synchronisation. En mode texte, il est en outre possible de confirmer individuellement les procédures de façon interactive.

Les utilisateurs expérimentés exécutent normalement subversion ou CVS à la ligne de commande. Il existe cependant des interfaces graphiques pour Linux, telles que cervisia ainsi que pour d'autres systèmes d'exploitation, comme wincvs. Beaucoup d'outils de

développement, tels que kdevelop, et d'éditeurs de texte, tels que emacs, offrent une prise en charge de CVS ou subversion. Ces interfaces frontales permettent bien souvent de résoudre plus facilement les conflits.

47.2.9 Convivialité

Unison et rsync sont assez faciles à utiliser et conviennent également aux débutants. CVS et subversion sont un peu plus complexes. Pour ces derniers, il faut avoir comprendre l'interaction entre le référentiel et les données locales. Les modifications des données doivent tout d'abord être comparées localement avec le référentiel. Les commandes `cvs update` et `svn update` sont prévues à cet effet. Les données doivent alors être renvoyées au référentiel avec les commandes `cvs commit` ou `svn commit`. Une fois qu'on a compris cette procédure, même les débutants peuvent facilement utiliser CVS ou subversion.

47.2.10 Sécurité contre les attaques

Dans le cas idéal, les données devraient être protégées contre l'interception et la manipulation. Unison, CVS, rsync et subversion s'utilisent facilement via ssh (secure shell) et sont ainsi sécurisés contre les attaques de ce genre. Il est préférable de ne exécuter CVS ou Unison via rsh (remote shell). De même, l'accès à CVS par le biais du mécanisme *pserver* est à déconseiller dans les réseaux non sécurisés. Grâce à l'utilisation d'Apache, subversion offre d'origine la sécurité nécessaire.

47.2.11 Sécurité contre la perte de données

Beaucoup de développeurs utilisent CVS depuis longtemps pour gérer leurs projets logiciels ; il est particulièrement stable. En enregistrant l'historique du développement, CVS offre même une protection contre certaines erreurs de l'utilisateur, telles que l'effacement accidentel d'un fichier. Bien que subversion ne bénéficie pas encore d'une aussi grande diffusion que CVS, on l'emploie déjà en productiion, par exemple pour le projet subversion lui-même.

Unison est encore relativement récent mais offre une grande stabilité. Il est toutefois plus sensible aux erreurs de l'utilisateur. Lorsqu'on en a terminé avec la synchronisation de l'effacement d'un fichier, celui-ci est irrémédiablement perdu.

Tableau 47.1 *Fonctionnalités des outils de synchronisation de fichiers : -- = très mauvais, - = mauvais ou non disponible, o = moyen, + = bon, ++ = excellent, x = disponible*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Client/Serveur	égale	C-S/C-S	C-S	égale
Portabilité	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interactivité	x	x/x	x	-
Vitesse	-	o/+	+	+
Conflits	o	++/++	o	+
Sél. de fichiers	Répertoire	Sél./fichier, rép.	Répertoire	Boîte aux lettres
Historique	-	x/x	-	-
Espace disque dur	o	--	o	+
Interf. util.	+	o/o	-	-
Complexité	+	o/o	+	o
Attaques	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Perte de donn.	+	++/++	+	+

47.3 Introduction à Unison

Unison convient particulièrement à la synchronsation et au transfert d'arborescence de répertoires complète. La synchronisation est bidirectionnelle et peut être contrôlée par une interface graphique intuitive. Bien entendu, vous pouvez aussi utiliser la version console. Il est également possible d'automatiser la synchronisation. Il n'y aura alors aucune interaction avec l'utilisateur mais ceci est à réserver aux utilisateurs expérimentés.

47.3.1 Conditions nécessaires

Unison doit être installé tant sur le client que sur le serveur. Dans ce contexte, le terme *serveur* désigne un deuxième ordinateur distant (contrairement à CVS, comme décrit dans la Section 47.1.2, « CVS » (p. 786)).

Dans la section suivante, nous nous limiterons à l'utilisation d'Unison avec ssh. Dans ce cas, un client SSH doit être installé sur le client et un serveur SSH sur le serveur.

47.3.2 Utilisation d'Unison

Le principe de base d'Unison est l'association de deux répertoires (*roots*). Cette association est de caractère symbolique, il ne s'agit pas d'une connexion en ligne. Supposons que le répertoire soit conçu de la manière suivante :

Client :	`/home/tux/rep1`
Serveur :	`/home/geeko/rep2`

Ces deux répertoires doivent être synchronisés. Sur le client, l'utilisateur est connu en tant que tux, tandis que sur le serveur il est connu en tant que `geeko`. On veut d'abord tester si la communication entre le client et le serveur fonctionne :

```
unison -testserver /home/tux/rep1 ssh://geeko@server//homes/geeko/rep2
```

Voici les problèmes les plus fréquents :

- les versions d'Unison utilisées sur le client et le serveur ne sont pas compatibles

- le serveur ne permet aucune connexion SSH
- aucun des deux chemins d'accès indiqués n'existe

Si tout se déroule bien, n'utilisez pas l'option `-testserver`. Lors de la synchronisation initiale, Unison ne connaît pas encore la relation entre les deux répertoires et fait donc des propositions pour le sens de transfert des différents fichiers et répertoires. Les flèches de la colonne *Action* indiquent le sens de transfert. Un point d'interrogation signifie qu'Unison ne peut pas faire de proposition concernant le sens du transfert parce que les deux versions ont été modifiées entre-temps ou sont nouvelles.

Le sens de transfert de chaque enregistrement peut être réglé avec les touches de direction (flèches). Si les sens de transfert de tous les enregistrements indiqués sont corrects, cliquez sur *Go*.

Le comportement d'Unison (par exemple, si la synchronisation doit s'effectuer automatiquement dans les cas sans équivoque) peut être contrôlé par des paramètres spécifiés en ligne de commande au démarrage du programme. Vous trouverez une liste complète de tous les paramètres dans `unison --help`.

Exemple 47.1 *Le fichier ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Pour chaque liaison, la synchronisation est consignée dans le répertoire utilisateur `~/.unison`. Dans ce répertoire, il est possible d'enregistrer des jeux de configuration tels que `~/.unison/example.prefs`. Pour lancer la synchronisation, il suffit tout simplement d'indiquer le fichier comme paramètre en ligne de commande comme dans : `unison example.prefs`.

47.3.3 Informations complémentaires

La documentation officielle d'Unison est très utile, cette section ne fournira donc qu'une brève introduction. Le manuel complet est disponible à l'adresse http://www.cis.upenn.edu/~bcpierce/unison/ et dans le paquetage `unison` de SUSE.

47.4 Introduction à CVS

CVS est adapté à la synchronisation s'il s'agit de fichiers individuels fréquemment modifiés et dont le format est un format de fichier tel que texte ASCII ou texte source de programme. L'utilisation de CVS pour la synchronisation de fichiers ayant un autre format, tels que les fichiers JPEG, est possible mais conduit très vite à de grandes quantités de données puisque chaque variante d'un fichier est enregistrée en permanence sur le serveur CVS. En plus, dans de tels cas, la plupart des possibilités offertes par CVS ne peuvent pas être utilisées. L'utilisation de CVS pour synchroniser des fichiers n'est possible que si tous les stations de travail peuvent accéder au même serveur.

47.4.1 Configuration d'un serveur CVS

Le *serveur* est le lieu où se trouvent tous les fichiers valables, notamment la dernière version de chaque fichier. Le serveur peut être un ordinateur de bureau fixe. Il est souhaitable que les données du serveur CVS soient régulièrement intégrées dans une sauvegarde.

Une bonne chose lors de la configuration d'un serveur CVS consiste à permettre à l'utilisateur d'accéder au serveur via SSH. Si, sur ce serveur, l'utilisateur est connu comme `tux` et si le logiciel CVS est installé sur le serveur ainsi que sur le client (ordinateur portable), il faut veiller, du côté du client, à ce que les variables d'environnement suivantes soient configurées :

```
CVS_RSH=ssh CVS_ROOT=tux@server:/repserveur
```

Avec la commande `cvs init`, le serveur CVS est ensuite initialisable du côté du client. Cela ne doit être effectué qu'une seule fois.

Enfin, il faut assigner un nom à la synchronisation. Sur un client, choisissez ou créez un répertoire ne contenant que des données qui seront administrées par CVS (le répertoire peut aussi être vide). Le nom du répertoire est également le nom de la synchronisation. Dans l'exemple présent, le répertoire est appelé `synchome`. Entrez dans ce répertoire et saisissez la commande suivante pour appeler la synchronisation `synchome` :

```
cvs import synchome tux wilber
```

Beaucoup de commandes de CVS requièrent un commentaire. A cet effet, CVS démarre un éditeur (celui qui est défini dans la variable d'environnement `$EDITOR` ou vi si aucun éditeur n'est défini). On peut éviter d'appeler un éditeur en entrant le commentaire à l'avance sur la ligne de commande, comme dans l'exemple suivant :

```
cvs import -m 'ceci est un Test' synchome  tux wilber
```

47.4.2 Utilisation de CVS

A partir de ce moment, il est possible de vérifier le référentiel de synchronisation depuis tous les ordinateurs à l'aide de : `cvs co synchome`. Il en résulte un nouveau sous-répertoire `synchome` sur le client. Si vous réalisez des modifications que vous voulez transmettre au serveur, entrez dans le répertoire `synchome` (ou dans un des ses sous-répertoires) et saisissez : `cvs commit`

Cela provoque, par défaut, la transmission au serveur de tous les fichiers (et sous-répertoires). Si on ne souhaite transmettre que des fichiers ou répertoires individuels, il faut les spécifier comme suit : `cvs commit fichier1 répertoire1` Avant leur transmission au serveur, il faut ajouter les nouveaux fichiers et répertoires au référentiel avec une commande telle que : `cvs add fichier1 répertoire1` Il faut ensuite les transmettre à l'aide de : `cvs commit fichier1 répertoire1`

Pour changer maintenant de poste de travail, il faut vérifier le référentiel de synchronisation, au cas où cela n'a pas encore été fait lors d'une session antérieure sur le même poste de (voir ci-dessus).

Démarrez la synchronisation avec le serveur avec la commande `cvs update`. Actualisez des fichiers ou répertoires avec `cvs update fichier1 répertoire1`. Pour voir les différences entre les fichiers actuels et les versions enregistrées sur le serveur, utilisez la commande `cvs diff` ou la commande `cvs diff fichier1 répertoire1`. Utilisez `cvs -nq update` pour voir quels fichiers ont été affectés par une mise à jour.

Voici certains des symboles d'état utilisés lors d'une mise à jour :

U

La version locale a été mise à jour. Ceci concerne tous les fichiers fournis par le serveur et qui manquent sur le système local.

M

La version locale a été modifiée. Si les modifications de la version ont eu lieu sur le serveur, les modifications ont pu être également exécutées localement.

P

La version locale a été corrigée avec la version du serveur.

C

Le fichier local entre en conflit avec la version actuelle du référentiel.

?

Ce fichier n'existe pas dans CVS.

L'état `M` marque un fichier localement modifié. Vous pouvez choisir d'envoyer le fichier local modifié au serveur ou de supprimer le fichier local et de procéder à une nouvelle actualisation. Dans ce cas, le fichier manquant est récupéré sur le serveur. Si vous synchronisez un fichier modifié localement et que ce fichier a été modifié au même endroit par plusieurs utilisateurs, cela peut provoquer un conflit lors d'une mise à jour. Ce cas de figure est marqué par le symbole `C`.

Dans ce cas, examinez le fichier correspondant au niveau des marques de conflits (»> et «<) et choisissez entre les deux versions. Ceci risquant d'être relativement pénible, vous pouvez choisir d'abandonner vos modifications en supprimant le fichier local et en saisissant `cvs up` pour récupérer la version actuelle du fichier sur le serveur.

47.4.3 Informations complémentaires

Cette section n'est qu'une petite introduction aux nombreuses possibilités de CVS. Vous trouverez une documentation plus complète sous :

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

47.5 Introduction à Subversion

Subversion est un système de contrôle de versions Open Source et est souvent considéré comme le successeur de CVS. Par conséquent, les propriétés déjà présentées de CVS s'appliquent aussi en grande partie à subversion. Il est surtout intéressant si l'on souhaite bénéficier des avantages de CVS sans avoir à en subir les inconvénients. Beaucoup de

ces propriétés ont déjà été présentées dans les grandes lignes dans la Section 47.1.3, « subversion » (p. 787).

47.5.1 Configuration d'un serveur Subversion

La configuration d'un référentiel sur un serveur est une procédure assez simple. Pour cela, subversion fournit un outil d'admnistration. Pour installer un nouveau référentiel, saisissez la commande :

```
svnadmin create /chemin/vers/le/referentiel
```

D'autres options sont disponibles via `svnadmin help`. Contrairement à CVS, subversion n'est pas basé sur RCS mais sur la base de données de Berkeley. Veillez à ne pas installer de référentiel sur des systèmes de fichiers distants tels que NFS, AFS ou Windows SMB. La base de données nécessite les mécanismes de verrouillage POSIX que les systèmes mentionnés ci-dessus ne prennent pas en charge.

Pour examiner le contenu d'un référentiel existant, utilisez la commande `svnlook`.

```
svnlook info /chemin/vers/le/referentiel
```

Pour que différents utilisateurs puissent accéder au référentiel, un serveur doit être configuré. Dans ce cas, on peut avoir recours au serveur Web Apache avec WebDAV ou utiliser le propre serveur de subversion, svnserve. Dès que svnserve fonctionne, on peut accéder au référentiel à l'aide de `svn://` ou `svn+ssh://` saisi dans un URL. Le fichier de configuration `/etc/svnserve.conf` vous permet de définir les utilisateurs qui doivent s'authentifier à l'invite de `svn`.

La décision pour Apache ou pour svnserve dépend de nombreux facteurs. Ici, un coup d'œil à l'ouvrage consacré à subversion s'impose. Vous trouverez plus d'informations à ce sujet dans la Section 47.5.3, « Informations complémentaires » (p. 800).

47.5.2 Utilisation

Pour accéder à un référentiel Subversion, il existe la commande `svn` (similaire à `cvs`). Si le serveur est correctement configuré (avec un référentiel correspondant), chaque client peut accéder à son contenu à l'aide de l'une des commandes suivantes :

```
svn list http://svn.example.com/chemin/vers/le/projet
```

ou

```
svn list svn://svn.example.com/chemin/vers/le/projet
```

Grâce à la commande `svn checkout`, vous pouvez enregistrer un projet existant dans le répertoire actuel :

```
svn checkout http://svn.example.com/chemin/vers/le/projet nom_du_projet
```

La validation crée un nouveau sous-répertoire `nom_du_projet` sur le client. On peut ainsi mettre en œuvre diverses modifications (ajout, copie, renommage, suppression) :

```
svn add fichier
svn copy ancien_fichier nouveau_fichier
svn move ancien_fichier nouveau_fichier
svn delete fichier
```

Chacune de ces commandes est applicable non seulement à des fichiers, mais aussi à des répertoires. De plus, subversion peut aussi attribuer ce que l'on appelle des propriétés à un fichier ou à un répertoire :

```
svn propset license GPL foo.txt
```

Dans l'exemple précédent concernant le fichier `foo.txt`, la propriété `license` se voit attribuer la valeur `GPL`. Grâce à `svn proplist`, vous pouvez afficher les propriétés :

```
svn proplist --verbose foo.txt
  Properties on 'foo.txt':
  license : GPL
```

Enregistrez les modifications sur le serveur avec `svn commit`. Pour qu'un autre utilisateur obtienne vos modifications dans son répertoire de travail, il doit procéder à une synchronisation avec le serveur à l'aide de la commande suivante `svn update`.

À la différence de CVS, l'état d'un répertoire de travail dans subversion peut être affiché *sans* avoir à accéder au référentiel avec la commande `svn status`. Dans ce cas, les modifications locales sont affichées dans cinq colonnes, la première colonne étant la plus importante :

''
: Aucune modification

'A'
: L'objet est à ajouter

'D'
: L'objet est à supprimer

'M'
: L'objet a été modifié

'C'
: L'objet est en situation de conflit

'I'
: L'objet a été ignoré

'?'
: L'objet n'est pas soumis au contrôle de versions

'!'
: L'objet est manquant. Cet indicateur apparaît si l'objet a été supprimé ou déplacé sans utiliser la commande `svn`.

'~'
: L'objet a été pris en charge comme fichier mais il a été, depuis lors, remplacé par un répertoire ou inversement.

La deuxième colonne indique l'état des propriétés. La signification de toutes les autres colonnes est consultable dans l'ouvrage consacré à subversion.

Utilisez la commande `svn help` pour obtenir la description d'un paramètre ou d'une commande :

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

47.5.3 Informations complémentaires

Le premier point de référence est la page d'accueil du projet subversion, sur le site `http://subversion.tigris.org`. Après l'installation du paquetage

subversion-doc, vous trouverez un livre en langue anglaise très intéressant et complet dans le répertoire file:///usr/share/doc/packages/subversion/html/book.html. Cet ouvrage est également disponible en ligne à l'adresse http://svnbook.red-bean.com/svnbook/index.html.

47.6 Introduction à rsync

rsync s'impose toujours quand il s'agit de transférer régulièrement de grandes quantités de données qui ne changent pas de façon trop considérable. C'est fréquemment le cas lorsqu'on met en place une sauvegarde par exemple. Un autre domaine d'application est ce que l'on appelle les staging servers (serveurs étape). Il s'agit de serveurs qui contiennent les arborescences complètes de serveurs Web et qui sont mis en miroir régulièrement sur un serveur Web dans une DMZ.

47.6.1 Configuration et utilisation

On peut utiliser rsync dans deux modes différents. D'une part, rsync peut archiver ou copier des fichiers. Pour cela, il suffit de faire appel à un shell distant comme par exemple ssh, sur le système cible. Cependant, rsync peut aussi être utilisé comme un démon pour fournir des répertoires au réseau.

L'utilisation principale de rsync n'exige aucune configuration particulière. Grâce à rsync, il est possible de mettre directement en miroir des répertoires complets sur un autre ordinateur. Par exemple, à l'aide de la commande suivante, on peut placer une sauvegarde du répertoire personnel de tux sur un serveur de sauvegarde sun :

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Pour restaurer le répertoire, utilisez la commande suivante :

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Jusqu'ici, l'utilisation se différencie à peine d'un programme normal de copie comme scp.

Afin que rsync puisse exploiter pleinement toutes ses fonctionnalités, il faudra l'utiliser en mode « rsync ». Pour ce faire, le démon rsyncd est démarré sur un des ordinateurs. Dans ce cas, rsync doit être configuré dans le fichier /etc/rsyncd.conf. Si par

exemple, il s'agit d'accéder au répertoire `/srv/ftp` via rsync, il est possible de faire appel au fichier de configuration suivant :

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Le démon rsyncd doit ensuite être démarré avec `rcrsyncd start`. Le démon rsyncd peut aussi être démarré automatiquement lors du processus d'amorçage. Pour cela, il faut activer ce service dans l'éditeur de niveau d'exécution de YaST ou saisir manuellement la commande `insserv rsyncd`. Il est également possible de démarrer rsyncd à partir de xinetd. Toutefois, ce n'est recommandé que pour les serveurs sur lesquels le rsyncd n'est pas trop souvent sollicité.

Dans notre exemple, un fichier journal est également créé pour toutes les connexions. Celui-ci est enregistré dans `/var/log/rsyncd.log`.

Maintenant, le transfert peut être testé depuis un ordinateur client. Cette opération a lieu à l'aide de la commande suivante :

```
rsync -avz sun::FTP
```

Cette commande permet de répertorier tous les fichiers présents sur le serveur dans le répertoire `/srv/ftp`. Cette requête est aussi enregistrée dans le fichier journal `/var/log/rsyncd.log`. Pour démarrer le transfert, indiquez un répertoire cible. Pour le répertoire actuel, utilisez « . ». Par exemple :

```
rsync -avz sun::FTP .
```

Par défaut, aucun fichier n'est supprimé lors de la synchonisation avec rsync. Lorsque la suppression doit être imposée, il faut indiquer l'option `--delete` en sus. Pour garantir qu'aucun fichier récent n'est écrasé, on peut indiquer l'option `--update` au lieu de `--delete`. Ainsi, les conflits qui en résultent doivent être résolus manuellement.

47.6.2 Informations complémentaires

Vous trouverez des informations importantes sur rsync dans les pages de manuel `man rsync` et `man rsyncd.conf`. Vous trouverez de la documentation technique sur les principes de fonctionnement de rsync dans `/usr/share/doc/packages/rsync/tech_report.ps`. Pour vous tenir informé sur rsync, vous pouvez consulter le site Web du projet à l'adresse `http://rsync.samba.org`.

47.7 Introduction à mailsync

En principe, Mailsync s'utilise pour les trois tâches suivantes :

- La synchronisation de courriers électroniques enregistrés localement avec des courriers électroniques enregistrés sur un serveur.
- La migration de boîtes aux lettres dans un format différent ou vers un autre serveur.
- Le contrôle de l'intégrité d'une boîte aux lettres ou la recherche de doubles.

47.7.1 Configuration et utilisation

Mailsync fait la distinction entre la boîte aux lettres elle-même (appelée *store*) et la liaison entre deux boîtes aux lettres (*channel*). Les définitions de stores et de channels sont enregistrées dans le fichier `~/.mailsync`. Vous trouverez ci-dessous la présentation de quelques exemples de stores.

Voici une définition simple :

```
store saved-messages {
   pat Mail/saved-messages
prefix  Mail/
}
```

`Mail/` est un sous-répertoire dans le répertoire personnel (/home) de l'utilisateur qui contient des dossiers de courrier électronique, dont entre autres le dossier `saved-messages`. En appelant `mailsync` via la commande `mailsync -m saved-messages`, vous obtenez un index de tous les messages contenus dans `saved-messages`. Si la définition suivante est donnée :

```
store localdir {
pat     Mail/*
prefix  Mail/
}
```

la commande `mailsync -m localdir` affiche une liste de tous les messages qui sont enregistrés sous `Mail/`. En revanche, la commande `mailsync localdir` affiche une liste des noms des dossiers. On spécifie un store sur un serveur IMAP ainsi :

```
store imapinbox {
server {mail.edu.harvard.com/user=gulliver}
ref    {mail.edu.harvard.com}
pat    INBOX
}
```

Dans ce cas de figure, seul le dossier principal est adressé sur le serveur IMAP ; un store pour les sous-dossiers ressemble à ceci :

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

Si le serveur IMAP supporte des liaisons chiffrées, il faudra modifier la spécification du serveur comme suit :

```
server {mail.edu.harvard.com/ssl/user=gulliver}
```

ou bien, si le certificat serveur n'est pas connu :

```
server {mail.edu.harvard.com/ssl/novalidate-cert/user=gulliver}
```

Le préfixe est expliqué plus tard.

Maintenant, on veut connecter les dossiers se trouvant sous `Mail/` aux sous-répertoires sur le serveur IMAP :

```
channel folder localdir imapdir {
msinfo .mailsync.info
}
```

mailsync utilise le fichier de `msinfo` pour conserver une trace des messages qui ont déjà été synchronisés.

La commande `mailsync dossier` a les conséquences suivantes :

- Le type de boîte aux lettres (pattern) est élargi des deux côtés.
- Le préfixe (prefix) résultant de chaque nom de dossier est éliminé.
- Les dossiers sont synchronisés (ou crées, s'ils n'existaient pas) par paires.

De même façon, le dossier `INBOX.sent-mail` sur le serveur IMAP est synchronisé avec le dossier local `Mail/sent-mail` (à condition de répondre aux définitions ci-dessus). La synchronisation entre les différents dossiers fonctionnent de la manière suivante :

- Si un message existe déjà des deux côtés, il ne se passe rien.
- Si le message manque d'un côté et s'il s'agit d'un nouveau message (non consigné dans le fichier de `msinfo`), il y sera transféré.
- Si le message n'existe que d'un côté et s'il s'agit d'un ancien message (déjà consigné dans le fichier de `msinfo`), il y sera effacé (étant donné qu'il existait auparavant de l'autre côté et qu'il y a été effacé).

Pour savoir d'avance quels messages seront transmis et lesquels seront effacés lors d'une synchronisation, on appelle mailsync avec un « channel » *et* un « store » avec : `mailsync dossier localdir`. Il en résulte une liste de tous les messages qui sont localement nouveaux ainsi qu'une liste de tous les messages qui seraient effacés du côté de IMAP lors d'une synchronisation. De la même façon, la commande `mailsync dossier imapdir` affiche une liste de tous les nouveaux messages du côté de IMAP ainsi qu'une liste de tous les messages qui seraient effacés localement lors d'une synchronisation.

47.7.2 Problèmes éventuels

Dans le cas d'une perte de données, la procédure la plus sûre est d'effacer le fichier de protocole du « channel » correspondant de `msinfo`. Il en résulte que tous les messages qui n'existent que d'un seul côté sont considérés comme nouveaux et seront transmis lors de la prochaine synchronisation.

Seuls les messages portant un identificateur message sont pris en compte par la synchronisation tandis que ceux n'ayant pas d'identificateur message sont tout simplement ignorés ; ils ne sont ni transmis ni effacés. Un identificateur de message manquant est normalement le résultat de programmes défectueux dans le processus de remise ou de génération du courrier.

Sur certains serveurs IMAP, le dossier principal est appelé par `INBOX` et les sous-dossiers sont appelés par un nom quelconque (contrairement à INBOX et INBOX.name). C'est la raison pour laquelle il n'est pas possible de spécifier un modèle exclusif de sous-dossiers pour de tels serveurs IMAP.

Les pilotes de boîtes aux lettres (c-client) qu'utilise mailsync placent, lorsque les messages ont été transmis sur un serveur IMAP, un drapeau d'état spécial, rendant impossible pour certains programmes de messagerie électronique, comme mutt, de reconnaître qu'un message est nouveau. Désactivez ce drapeau d'état spécial avec l'option `-n`.

47.7.3 Informations complémentaires

Le fichier `README` contenu dans le paquetage `mailsync` contient des informations et conseils supplémentaires. Dans ce contexte, le RFC 2076 « Common Internet Message Headers » est particulièrement intéressant.

Samba 48

Samba permet de configurer une machine Unix comme serveur de fichiers ou d'impression pour des ordinateurs DOS, Windows et OS/2. Samba est devenu un produit à part entière assez complexe. Ce chapitre décrit les fonctionnalités de base du produit, ainsi que les principes essentiels de configuration et les modules YaST qui permettent de configurer Samba sur votre réseau.

Vous trouverez des informations détaillées sur Samba dans la documentation numérique. Entrez `apropos samba` dans la ligne de commande pour afficher des pages de manuel ou parcourez simplement le répertoire `/usr/share/doc/packages/samba`, si Samba est installé, pour obtenir d'autres exemples et documents en ligne. Vous trouverez un exemple de configuration détaillé (`smb.conf.SuSE`) dans le sous-répertoire `examples`.

Voici les principales nouvelles fonctionnalités de la version 3 du paquetage `samba` :

- Prise en charge d'Active Directory
- Meilleure prise en charge d'Unicode
- Refonte des mécanismes d'authentification internes
- Meilleure prise en charge du système d'impression Windows 200x et XP
- Possibilité de configuration des serveurs en tant que serveurs membres des domaines Active Directory

- Adoption d'un domaine NT4, qui permet de migrer d'un domaine NT4 à un domaine Samba

ASTUCE: Migration vers Samba 3

Vous devez tenir compte de certains facteurs lorsque vous migrez de Samba 2.x à Samba 3. Un chapitre complet est consacré à ce sujet dans l'ensemble des HOWTO (Guides pratiques) relatifs à Samba. Une fois le paquetage `samba-doc` installé, vous trouverez le HOWTO (Guide pratique) dans `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Samba utilise le protocole SMB (Server Message Block), qui est basé sur les services NetBIOS. Face aux pressions de la société IBM, Microsoft a publié le protocole, ce qui a permis à d'autres éditeurs de logiciels de se connecter également à un domaine Microsoft. Avec Samba, le protocole SMB fonctionne sur le protocole TCP/IP, qui doit donc être installé sur tous les clients.

NetBIOS est une interface logicielle (API) qui permet aux ordinateurs de communiquer entre eux. C'est dans ce contexte qu'un service de noms est fourni. Il permet aux machines connectées au réseau de se réserver des noms. Une fois la réservation effectuée, vous pouvez appeler ces machines par leur nom. Aucun processus central ne vérifie les noms. Toute machine du réseau peut réserver autant de noms qu'elle le souhaite, à condition qu'ils ne soient pas déjà utilisés. Vous pouvez désormais implémenter l'interface NetBIOS dans différentes architectures réseau. NetBEUI est une implémentation qui fonctionne de façon assez semblable au matériel réseau. On l'appelle généralement NetBIOS. Les protocoles réseau implémentés avec NetBIOS sont IPX de Novell (NetBIOS via TCP/IP) et TCP/IP.

Les noms NetBIOS envoyés via TCP/IP n'ont rien à voir avec les noms utilisés dans `/etc/hosts`, ni avec ceux définis par DNS. NetBIOS utilise sa propre convention de dénomination, qui est totalement indépendante. Il est toutefois recommandé d'utiliser des noms qui correspondent aux noms d'hôte DNS afin de faciliter l'administration. C'est d'ailleurs le paramètre par défaut utilisé par Samba.

Tous les systèmes d'exploitation classiques, tels que Mac OS X, Windows et OS/2, prennent en charge le protocole SMB. Le protocole TCP/IP doit être installé sur tous les ordinateurs. Samba fournit un client pour les différentes variantes UNIX. Sous Linux, un module de kernel pour SMB permet d'intégrer des ressources SMB au niveau du système Linux.

Les partages permettent aux serveurs SMB de fournir de l'espace disque à leurs clients. Un partage correspond à un répertoire et à tous ses sous-répertoires sur le serveur. Vous pouvez l'exporter sous son propre nom et y accéder avec ce même nom. Le nom du partage peut être choisi librement (il ne doit pas nécessairement être identique à celui du répertoire exporté). Un nom est également assigné à l'imprimante. Les clients utilisent ce nom pour accéder à l'imprimante.

48.1 Configuration du serveur

Si vous souhaitez utiliser Samba comme serveur, installez `samba`. Utilisez la commande `rcnmb start && rcsmb start` pour démarrer les services requis pour Samba et la commande `rcsmb stop && rcnmb stop` pour les arrêter.

Le principal fichier de configuration de Samba est `/etc/samba/smb.conf`. Ce fichier est divisé en deux parties logiques. La section `[global]` contient les paramètres généraux. Les sections `[share]` contiennent les différents partages de fichiers et d'imprimantes. Ce mode d'organisation permet de définir les détails des partages soit de manière différenciée, soit avec une portée globale dans la section `[global]`. Le fichier de configuration gagne ainsi en lisibilité.

48.1.1 Section global

Vous devez adapter les paramètres suivants de la section `[global]` à la configuration de votre réseau, afin que les autres machines puissent accéder à votre serveur Samba via SMB dans un environnement Windows.

workgroup = TUX-NET

Cette ligne assigne le serveur Samba à un groupe de travail. Remplacez `TUX-NET` par le groupe de travail souhaité de votre environnement réseau. Votre serveur Samba apparaît sous son nom DNS, sauf si celui-ci a été assigné à une autre machine du réseau. Si le nom DNS n'est pas disponible, définissez le nom du serveur à l'aide de `netbiosname=MON NOM`. Pour plus d'informations sur ce paramètre, consultez la commande `man smb.conf`.

os level = 2

Ce paramètre détermine si votre serveur Samba tente de devenir LMB (Local Master Browser) pour son groupe de travail. Choisissez une valeur très faible pour éviter

que le réseau Windows existant soit perturbé par un serveur Samba mal configuré. Pour plus d'informations sur ce sujet important, consultez les fichiers `BROWSING.txt` et `BROWSING-Config.txt` situés dans le sous-répertoire `textdocs` de la documentation du paquetage.

Si votre réseau ne comporte aucun autre serveur SMB (tel qu'un serveur Windows NT ou 2000) et si vous souhaitez que le serveur Samba conserve une liste de tous les systèmes présents dans l'environnement local, affectez à `os level` une valeur supérieure (par exemple, `65`). Votre serveur Samba est alors choisi comme LMB de votre réseau local.

Si vous modifiez ce paramètre, soyez particulièrement attentif aux éventuelles répercussions sur un environnement réseau Windows existant. Commencez par tester les modifications dans un réseau isolé ou pendant une période non critique.

prise en charge wins et serveur wins

Pour intégrer votre serveur Samba dans un réseau Windows existant avec un serveur WINS actif, activez l'option `Serveur WINS` et affectez-lui l'adresse IP de ce serveur WINS.

Si vos machines Windows sont connectées à des sous-réseaux distincts mais doivent se reconnaître entre elles, vous devez configurer un serveur WINS. Pour transformer un serveur Samba en serveur WINS de ce type, définissez l'option `wins support = Yes`. Assurez-vous que ce paramètre n'est activé que pour un seul serveur Samba du réseau. Les options `wins server` et `wins support` ne doivent jamais être activées simultanément dans votre fichier `smb.conf`.

48.1.2 Partages

Les exemples suivants illustrent le partage d'un lecteur CD-ROM et de répertoires d'utilisateurs (`homes`) entre des clients SMB.

[cdrom]

Pour éviter que le lecteur de CD ne soit partagé par inadvertance, ces lignes sont désactivées à l'aide de marques de commentaires (des points-virgules, en l'occurrence). Supprimez les points-virgules de la première colonne pour partager le lecteur de CD avec Samba.

Exemple 48.1 Partage de CD

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` et `comment`
: L'entrée `[cdrom]` correspond au nom du partage que voient tous les clients SMB du réseau. Vous pouvez ajouter une déclaration `comment` pour fournir une description plus détaillée du partage.

`path = /media/cdrom`
: `path` exporte le répertoire `/media/cdrom`.

Ce type de partage est uniquement disponible pour les utilisateurs présents sur ce système, en raison d'une configuration par défaut très restrictive. Si vous souhaitez que tout le monde puisse accéder à ce partage, ajoutez la ligne `guest ok = yes` à la configuration. Ce paramètre octroie des autorisations de lecture à toute personne se trouvant sur le réseau. Il est recommandé d'utiliser ce paramètre avec la plus grande prudence. Cette recommandation s'applique encore plus à l'utilisation de ce paramètre dans la section `[global]`.

`[homes]`
: Le partage `[home]` est particulièrement important. Si l'utilisateur possède un compte et un mot de passe valides pour le serveur de fichiers Linux et son propre répertoire privé, il peut se connecter à ce compte.

Exemple 48.2 Partage homes

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]
: Tant qu'aucun autre partage n'utilise le nom de partage de l'utilisateur connecté au serveur SMB, un partage est généré de façon dynamique à l'aide des directives de partage `[homes]`. Le nom du partage obtenu est le nom de l'utilisateur.

valid users = %S

Une fois la connexion établie, `%S` est remplacé par le nom de partage réel. Dans le cas d'un partage `[homes]`, il s'agit toujours du nom d'utilisateur. Par conséquent, les droits d'accès au partage d'un utilisateur sont exclusivement limités à l'utilisateur.

browseable = No

Ce paramètre rend le partage invisible dans l'environnement réseau.

read only = No

Par défaut, Samba interdit l'accès en écriture à tout partage exporté à l'aide du paramètre `read only = Yes`. Pour autoriser l'accès en écriture à un partage, choisissez la valeur `read only = No`, qui est équivalente à `writeable = Yes`.

create mask = 0640

Les systèmes qui ne sont pas basés sur MS Windows NT ne connaissent pas le concept des autorisations Unix. Ils ne peuvent donc pas assigner d'autorisations lors de la création d'un fichier. Le paramètre `create mask` définit les autorisations d'accès assignées aux nouveaux fichiers. Cette fonctionnalité ne concerne que les partages accessibles en écriture. En effet, ce paramètre signifie que le propriétaire possède des autorisations de lecture et d'écriture et que les membres du groupe principal du propriétaire bénéficient d'autorisations de lecture. `valid users = %S` interdit l'accès en lecture, même si le groupe possède des autorisations de lecture. Pour accorder au groupe une autorisation de lecture ou d'écriture, désactivez la ligne `valid users = %S`.

48.1.3 Niveaux de sécurité

Le protocole SMB, issu de l'environnement DOS et Windows, se charge directement du problème de la sécurité. Tout accès à un partage peut être protégé par mot de passe. SMB peut vérifier les autorisations de trois manières :

Sécurité au niveau du partage (security = share) :

Un mot de passe est strictement assigné à un partage. Toute personne connaissant ce mot de passe peut accéder au partage.

Sécurité au niveau de l'utilisateur (security = user) :

Cette variante introduit le concept de l'utilisateur dans SMB. Chaque utilisateur doit s'enregistrer sur le serveur à l'aide d'un mot de passe. Une fois l'utilisateur enregistré, le serveur peut accorder l'accès aux différents partages exportés en fonction des noms d'utilisateur.

Sécurité au niveau du serveur (security = server) :

Pour les clients, Samba travaille en mode sécurité au niveau de l'utilisateur. Il transmet toutefois toutes les demandes de mot de passe à un autre serveur qui assure l'authentification en mode sécurité au niveau de l'utilisateur. Cette configuration exige un paramètre supplémentaire (`password server =`).

La distinction entre sécurité au niveau du partage, de l'utilisateur et du serveur concerne l'ensemble du serveur. Il est donc impossible que certains partages d'un serveur configuré offrent une sécurité au niveau du partage tandis que d'autres offrent une sécurité au niveau de l'utilisateur. Vous pouvez toutefois exécuter un serveur Samba distinct pour chaque adresse IP configurée sur un système.

Pour plus d'informations à ce sujet, consultez l'ensemble des HOWTO (Guides pratiques) de Samba. Si un système comporte plusieurs serveurs, accordez une attention particulière aux options `interfaces` et `bind interfaces only`.

ASTUCE

Vous pouvez également utiliser le programme swat pour les tâches simples d'administration du serveur Samba. Il comporte une interface Web conviviale, qui vous permet de configurer facilement le serveur Samba. Dans un navigateur Web, tapez l'adresse `http://localhost:901`, puis loguez-vous en tant qu'utilisateur `root`. Vous devez également activer swat dans les fichiers `/etc/xinetd.d/samba` et `/etc/services`. Dans `/etc/xinetd.d/samba`, remplacez la ligne `disable` par `disable = no`. Pour plus d'informations sur le programme swat, consultez la page du manuel correspondante.

48.2 Samba utilisé comme serveur de login

Dans les réseaux comportant essentiellement des clients Windows, il est généralement souhaitable de permettre uniquement aux utilisateurs disposant d'un compte et d'un mot de passe valides de s'enregistrer. Le serveur Samba offre cette possibilité. Dans un réseau basé sur Windows, cette tâche est assurée par un serveur Windows NT configuré en tant que contrôleur de domaine principal. Les lignes à ajouter à la section `[global]` du fichier `smb.conf` apparaissent dans l'Exemple 48.3, « Section Global dans smb.conf » (p. 814).

Exemple 48.3 *Section Global dans smb.conf*

```
[global]
  workgroup = TUX-NET
  domain logons = Yes
  domain master = Yes
```

Si vous utilisez des mots de passe codés à des fins de vérification (paramètre par défaut dans les installations MS Windows 9x, MS Windows NT 4.0 du Service Pack 3 et tous les produits plus récents correctement mis à jour), le serveur Samba doit être capable de les gérer. C'est le rôle de la ligne `encrypt passwords = yes` dans la section `[global]` (option par défaut dans Samba version 3). Il est également nécessaire de préparer des comptes utilisateur et des mots de passe dans un format de codage adapté à Windows. Pour ce faire, utilisez la commande `smbpasswd -a nom`. Créez le compte de domaine des ordinateurs, requis par le concept de domaine Windows NT, à l'aide des commandes suivantes :

Exemple 48.4 *Configuration d'un compte machine*

```
useradd hostname\$
smbpasswd -a -m hostname
```

La commande `useradd` permet d'ajouter le symbole $. Si vous utilisez le paramètre `-m` , la commande `smbpasswd` insère automatiquement ce symbole. L'exemple de configuration fourni (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) contient les paramètres qui automatisent cette tâche.

Exemple 48.5 Configuration automatique d'un compte machine

```
add machine script = /usr/sbin/useradd -g nogroup -c "Compte machine NT" \
-s /bin/false %m\$
```

Pour être sûr que Samba exécute ce script correctement, choisissez un utilisateur Samba doté des autorisations administrateur requises. Pour ce faire, sélectionnez un utilisateur et ajoutez-le au groupe `ntadmin`. Une fois cette opération effectuée, vous pouvez assigner l'état `Domain Admin` à tous les utilisateurs appartenant à ce groupe Linux, à l'aide de la commande suivante :

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

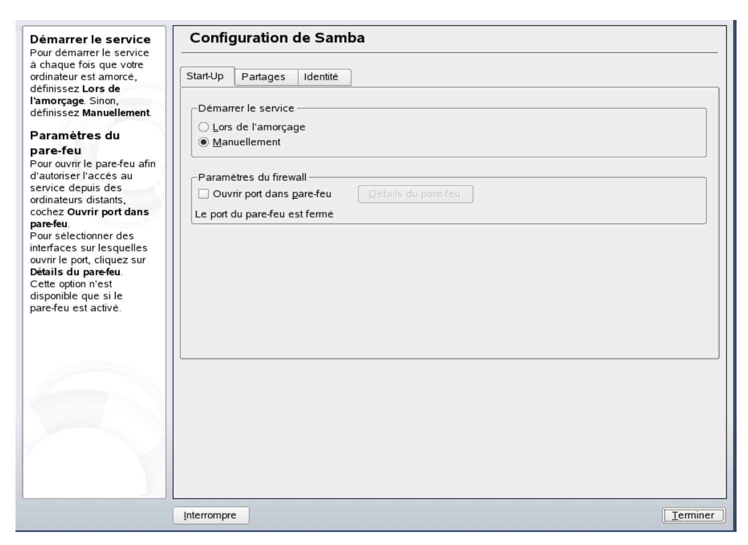
Pour plus d'informations à ce sujet, consultez le chapitre 12 de l'ensemble HOWTO (Guides pratiques) de Samba, que vous trouverez dans le fichier `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

48.3 Configuration d'un serveur Samba avec YaST

Pour démarrer la configuration du serveur, sélectionnez le groupe de travail ou le domaine que votre nouveau serveur Samba doit contrôler. Utilisez la liste *Groupe de travail ou nom de domaine* ou saisissez-en un nouveau. L'étape suivante vous permet d'indiquer si votre serveur doit tenir le rôle de contrôleur de domaine principal ou de contrôleur de domaine de secours.



***Figure 48.1** Configuration de Samba - Démarrage*



Activez Samba dans l'onglet de *démarrage* illustré à la Figure 48.1, « Configuration de Samba - Démarrage » (p. 816). Utilisez les options *Ouvrir port dans pare-feu* et *Détails du pare-feu* pour adapter le pare-feu sur le serveur de façon à ce que les ports des services `netbios-ns`, `netbios-dgm`, `netbios-ssn` et `microsoft-ds` soient ouverts sur toutes les interfaces externes et internes, afin de garantir le bon fonctionnement du serveur Samba.

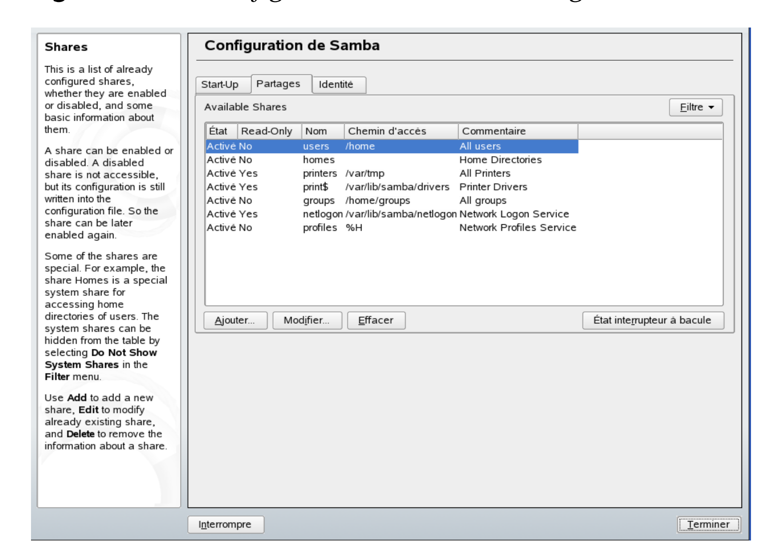


Figure 48.2 *Configuration de Samba - Partages*

Dans *Partages* (Figure 48.2, « Configuration de Samba - Partages » (p. 817)), déterminez les partages Samba à activer. Utilisez l'option *État de l'interrupteur à bascule* pour passer de l'état *actif* à l'état *inactif* et inversement. Cliquez sur *Ajouter* pour ajouter de nouveaux partages.

***Figure 48.3** Configuration de Samba - Identité*

L'onglet *Identité*, illustré à la Figure 48.3, « Configuration de Samba - Identité » (p. 818), permet d'indiquer le domaine auquel est associé l'hôte (*Paramètres de base*) et de déterminer si un autre nom d'hôte doit être utilisé dans le réseau (*Nom d'hôte NetBIOS*).

48.4 Configuration des clients

Seul le protocole TCP/IP permet aux clients d'accéder au serveur Samba. Les protocoles NetBEUI et NetBIOS via IPX ne peuvent pas être utilisés avec Samba.

48.4.1 Configuration d'un client Samba avec YaST

Configurez un client Samba pour accéder aux ressources (fichiers ou imprimantes) du serveur Samba. Saisissez le domaine ou le groupe de travail dans la boîte de dialogue *Groupe de travail SAMBA*. Cliquez sur *Parcourir* pour afficher tous les groupes et domaines disponibles, que vous pouvez sélectionner avec la souris. Si vous activez l'option *Utiliser également les informations SMB pour l'authentification Linux*,

l'authentification utilisateur est exécutée sur le serveur Samba. Après avoir défini tous les paramètres, cliquez sur *Terminer* pour achever la configuration.

48.4.2 Windows 9x et ME

Windows 9x et ME disposent déjà de la prise en charge intégrée de TCP/IP. Elle n'est toutefois pas installée par défaut. Pour ajouter le protocole TCP/IP, cliquez sur *Panneau de configuration* → *Système*, puis sélectionnez *Ajouter* → *Protocoles* → *TCP/IP Microsoft*. Après avoir redémarré la machine, vous trouverez le serveur Samba en double-cliquant sur l'icône du bureau représentant l'environnement réseau.

ASTUCE

Pour utiliser une imprimante sur le serveur Samba, installez le pilote d'impression standard ou Apple-PostScript à partir de la version Windows correspondante. Il est préférable de se connecter à la file d'attente d'impression Linux, qui accepte le format PostScript en entrée.

48.5 Optimisation

`socket options` est l'une des optimisations possibles proposées par l'exemple de configuration qui accompagne votre version de Samba. Sa configuration par défaut fait référence à un réseau Ethernet local. Pour plus d'informations sur `socket options`, consultez la section correspondante des pages du manuel portant sur `smb.conf` et la page du manuel sur `socket(7)`. Vous trouverez des informations complémentaires dans le chapitre consacré au réglage des performances de Samba de l'ensemble HOWTO (Guides pratiques).

La configuration standard de `/etc/samba/smb.conf` est conçue pour fournir des paramètres utiles basés sur la configuration par défaut de l'équipe Samba. Pour autant, il n'est pas possible de mettre au point une configuration « toute faite », notamment en ce qui concerne la configuration du réseau et le nom du groupe de travail. L'exemple de configuration fourni (`examples/smb.conf.SuSE`) contient des informations utiles pour l'adaptation aux exigences locales.

ASTUCE

L'ensemble HOWTO (Guides pratiques) de Samba fourni par l'équipe Samba comporte une section sur le dépannage. En outre, la partie V du document décrit en détail la marche à suivre pour vérifier votre configuration.

Index

Symboles

écran
  résolution, 569
éditeurs
  Emacs, 501–502
  vi, 448
édition d'images
  Digikam, 228

A

ACL, 377–388
  accès, 378, 382
  algorithme de contrôle, 387
  bits d'autorisation, 380
  définitions, 378
  effets, 384
  gestion, 379
  masques, 383
  par défaut, 378, 384
  prise en charge, 387
  structure, 379
adresses
  IP, 609
adresses IP
  assignation dynamique, 691
  IPv6, 612
    configuration, 620
  masquage, 344
  privées, 611
adresses IP
  classes, 609
agendas
  Evolution, 173, 180
  Kontact, 188, 196
aide
  OpenOffice.org, 169
  pages d'informations, 501
  pages de manuel, 435, 501
  X, 571
alevt, 144
alsamixer, 121
amaroK, 125
amorçage
  clés USB, 472
  configuration
    YaST, 484–490
  gestionnaires d'amorçage, 472
  graphique, 491
  GRUB, 473–494
  initramfs, 455
  initrd, 455
  secteurs d'amorçage, 471–472
  systèmes d'exploitation multiples, 472
Apache
  apxs2, 746
  arrêt, 761
  configuration, 747
    AccessFileName, 759
    activation, 761
    AllowOverride, 757
    DirectoryIndex, 757
    ErrorLog, 759
    httpd.conf, 756–757
    hôtes virtuels, 760
    LoadModule, 756
    LogLevel, 760
    manuelle, 754
    module Apache YaST, 747
  domaine, 738
  démarrage, 761
  dépannage, 781
  en-tête et fichiers d'inclusion, 746
  fichiers binaires, 743
  fichiers de configuration, 744
  fichiers journaux, 745
  hôtes virtuels, 763

alias IP, 766
à base d'adresse IP, 766
à base de nom, 763
installation, 739
module prefork MPM, 742
module worker MPM, 742
modules, 740
YaST, 740
modules, 767
extension, 771
modules externes, 775
Modules
Modules de base, 768
protocoles
FTP, 738
HTTP, 738
HTTPS, 738
SSL
configuration, 754
sécurité, 779
terminologie, 737
appareils photo numériques, 217–237, 267
accès, 218
connexion, 217
Digikam, 219–228
f-spot, 229
Konqueror, 219
protocole PTP, 218
applications
bureau
Evolution, 171
bureautique
Kontact, 185
OpenOffice.org, 161
graphiques
Digikam, 219
GIMP, 247
images
Kooka, 239
Linphone, 95
multimédias
amaroK, 125
audacity, 136
Grip, 133
K3b, 151
KMix, 120
KsCD, 131
XMMS, 129
réseau
Evolution, 171
Firefox, 85
Konqueror, 79
Kontact, 185
applications de messagerie
Kontact, 185–200
applications de messagerie électronique
Evolution, 171–183
arecord, 139
assistance à l'installation
cartes graphiques 3D et, 580
assistants numériques personnels (PDA)
Evolution, 182
Kontact, 198
Assistants personnels
KPilot, 201–208
assistants personnels, 268
audacity, 136
authentification
PAM, 581–589
autorisations, 429–434
ACL, 377–388
affichage, 429
autorisations de fichiers, 498
changement, 438
fichiers, 429
listes de contrôle d'accès, 434
modification, 431
répertoires, 431
systèmes de fichiers, 429
autorisations d'accès (voir autorisations)

B

Bash, 417–428
- .bashrc, 496
- .profile, 496
- caractères jokers, 424
- commandes, 418
- fonctions, 421
- profile, 495
- tuyaux, 425

BIND, 663–673
Bluetooth, 265, 322
- hciconfig, 329
- hcitool, 328
- opd, 331
- pand, 330
- réseau, 326
- sdptool, 329

bzip2, 427

C

cartes
- graphiques, 570
- réseau, 623

cat, 441
CD
- amorçage depuis, 472
- copie, 155
- création, 151–158
  - audio, 154
  - données, 151
- extraction (RIP), 131–135
- images ISO, 156
- lecteurs, 131
- lecture, 131–135
- multisession, 157

cd, 437
CD Text, 155
chemins, 423
- absolus, 423
- relatifs, 423
- utilisation des, 423

chgrp, 432, 438
chiffrement, 107–115
chmod, 431, 438
chown, 432, 437
CJK, 504
clavier
- affectation, 503
  - composition, 503
  - séquence de touches, 503
- caractères asiatiques, 504
- configuration, 503
- extension X Keyboard, 503
- XKB, 503

clear, 447
codage
- configuration avec YaST, 359
- création de partitions, 360–361
- Evolution, 175
- fichiers, 358, 361
- fichiers avec vi, 361
- ISO-8859-1, 506
- Kontact, 191
- partitions, 358
- support amovible, 362

coldplug, 540
commandes, 435–447
- bzip2, 427
- cat, 441
- cd, 437
- chgrp, 432, 438
- chmod, 431, 438
- chown, 432, 437
- clear, 447
- cp, 436
- date, 444
- df, 443
- diff, 442
- du, 444

fonts-config, 572
free, 444, 500
getfacl, 382
grep, 441
grub, 473
gzip, 427, 439
halt, 447
help, 418
hotplug, 537
kill, 445
killall, 445
ldapdelete, 724
ldapmodify, 723
ldapsearch, 723
less, 441
ln, 437
locate, 440
lp, 520
ls, 436
man, 435
mkdir, 437
mount, 442
mv, 436
nslookup, 446
passwd, 447
ping, 446
ps, 445
reboot, 447
rm, 437
rmdir, 437
scp, 354
setfacl, 382
sftp, 354
slptool, 653
smbpasswd, 814
ssh, 353
ssh-keygen, 356
su, 447
tar, 426, 439
telnet, 446
top, 445
udev, 543
umount, 443
updatedb, 440
commands
find, 441
ldapadd, 721
ssh-agent, 357
configuration, 466
DSL, 632
GRUB, 473, 481
impression, 513–516
IPv6, 620
IrDA, 335
modem câble, 632
modems, 626
RNIS, 629
routage, 639
réseaux, 623
manuelle, 635–646
Samba, 809–813
clients, 818
SSH, 352
T-DSL, 634
Configuration
DNS, 655
connexions sans fil
Bluetooth, 322
consignation
logrotate
configuration, 498
consoles
attribution, 503
changement, 502
graphique, 491
courrier électronique
synchronisation, 787
mailsync, 803–806
cp, 436
cpuspeed, 297

cron, 496
CVS, 786, 795–797

D

date, 444
df, 443
DHCP, 691–701
  assignation d'une adresse statique, 699
  configuration avec YaST, 692
  dhcpd, 697–698
  paquetages, 696
  serveur, 697–698
diff, 442
Digikam, 219–228
  édition d'images, 228
disques
  amorçage
    créer, 490
disques d'amorçage, 472
  CD, 472
disquettes
  amorçage depuis, 472
DNS, 621
  analyse des problèmes, 664
  BIND, 663–673
  configurer, 655
  domaine de niveau supérieur, 622
  domaines, 640
  démarrer, 664
  journalisation, 668
  NIC, 622
  notions de base, 655
  options, 666
  redirection (forwarding), 664
  résolution inverse, 672
  serveur de messagerie (MX - Mail Exchanger), 622
  serveurs de noms, 640
  sécurité, 372
  zones
    fichiers, 669
DOS
  partage de fichiers, 807
du, 444
démarrage, 453
  GRUB, 471
désinstallation
  GRUB, 490
  Linux, 490

E

Emacs, 501–502
  .emacs, 501
  default.el, 502
Evolution, 171–183, 268
  agenda, 173, 180
  assistants numériques personnels (PDA) et, 182
  carnets d'adresses, 178
  codage, 175
  comptes, 174
  contacts, 173, 178
  création de messages, 175
  dossiers, 176
  démarrage, 171
  Exchange, 171, 180, 182
  filtres, 177
  Groupwise, 180, 182
  importation de messages, 171
  pièces jointes, 175
  signature, 175
  tâches, 173
extension X Keyboard (voir clavier, XKB)

F

f-spot, 229
fichiers
  affichage, 425, 441

archivage, 426, 439
chemins, 423
chiffrement, 114
codage, 358
comparaison, 442
compression, 426, 439
conversion à partir de formats Microsoft, 162
copie, 436
décompression, 427
déplacement, 436
formats
GIF, 253
JPG, 252
PAT, 252
PNG, 253
XCF, 252
recherche, 499
recherche de, 440–441
recherche de contenu, 441
shell, 422
suppression, 437
synchronisation, 785–806
CVS, 786, 795–797
mailsync, 787, 803–806
rsync, 788
subversion, 787
Unison, 786, 793–794
Windows, 162
fichiers core, 499
fichiers de configuration, 638
.bashrc, 496, 499
.emacs, 501
.mailsync, 803
.profile, 496
.xsession, 357
/etc/fstab, 442
acpi, 289
autorisations, 373
crontab, 496
csh.cshrc, 506
dhclient.conf, 696
dhcp, 639
dhcpd.conf, 697
exports, 689–690
grub.conf, 481
host.conf, 642
HOSTNAME, 645
hotplug, 536
hwup, 538
hôtes, 622, 641
ifcfg-*, 638
inittab, 457, 459–460, 503
inputrc, 503
irda, 335
kernel, 455
langue, 504, 506
logrotate.conf, 498
menu.lst, 474
nscd.conf, 645
nsswitch.conf, 643, 725
pam_unix2.conf, 724
powersave, 289
profil, 506
profile, 495, 499
resolv.conf, 501, 640
routes, 639
réseau, 639
réseaux, 641
samba, 813
services, 813
slapd.conf, 715
smb.conf, 807, 809
smppd.conf, 647
smpppd-c.conf, 648
sshd_config, 358
suseconfig, 469
sysconfig, 466–469
termcap, 503
wireless, 639

xorg.conf, 565
Device, 569
Monitor, 570
Screen, 568
Fichiers de configuration
named.conf, 663, 665–673
resolv.conf, 663
fichiers de journalisation
XFree86, 579
fichiers journaux, 497
boot.msg, 289
messages, 351
Unison, 794
Fichiers journaux
messages, 664
filtres de paquets (voir pare-feux)
find, 441
Firefox, 85–94
configuration, 90
démarrage, 85
extensions, 90
gestionnaire de téléchargements, 90
impression, 93
marque-pages, 87
gestion, 88
migration, 89
navigation, 85
onglets, 86
panneau latéral, 86
recherche avec, 87, 92
recherche dans la page, 87
thèmes, 91
Firewire (IEEE1394)
disques durs, 267
free, 444

G

gestion de l'alimentation, 260, 285–297
ACPI, 285, 288–295
APM, 285, 287–288
attente, 286
hibernation, 286
moniteur de charge de la batterie, 286
veille, 286
gestion de l'énergie, 297–306
ACPI, 301
APM, 301
cpufrequency, 297
cpuspeed, 297
niveau de charge, 301
powersave, 297
YaST, 306
Gestionnaire de volumes logiques (voir LVM)
gestionnaires de téléchargements
Firefox, 90
GIMP, 247–255
configuration, 248
création d'images, 250
démarrage, 248
enregistrement d'images, 252
impression, 253
modèles, 250
ouverture d'images, 251
vues, 251
GNOME
lecteur de CD, 132
son, 120
GNU, 417
gphoto2, 217
graphique
3D, 577–580
3Ddiag, 579
assistance à l'installation, 580
diagnostic, 579
dépannage, 579
pilote, 577
prise en charge, 577
SaX, 578

tester, 579
cartes
3D, 577–580
GLIDE, 577–580
OpenGL, 577–580
pilote, 577
tester, 579
graphiques
albums, 222
appareils photo numériques, 217
cartes
pilotes, 570
en pixels, 247
f-spot, 229
formats de fichier, 252
modification, 247–255
vectoriels, 247
édition (de base), 228
grep, 441
Grip, 133
GroupWise, 198
conseils, 199
différences terminologiques, 198
GRUB, 471–494
amorçage, 473
caractères joker, 480
commandes, 473–484
device.map, 474, 481
dépannage, 492
désinstallation, 490
erreur GRUB Geom, 493
grub.conf, 474, 481
JFS et GRUB, 493
limites, 473
MBR (Master Boot Record - secteur d'amorçage principal), 471
menu d'amorçage, 474
menu.lst, 474
mot de passe d'amorçage, 483
noms de partition, 476
noms de périphérique, 476
secteurs d'amorçage, 472
shell GRUB, 482
systèmes d'exploitation multiples et, 472
éditeur de menu, 479
gunzip, 427
gzip, 427, 439

H

halt, 447
hciconfig, 329
hcitool, 328
hotplug, 535–541
agent, 538
analyse des erreurs, 540
configuration
interfaces, 538
périphériques, 538
enregistreur d'événements, 541
fichiers journaux, 540
hwcfg, 540
modules, 540
nom des périphériques, 536
périphériques de stockage, 539
périphériques réseau, 538
événements, 537

I

I18N, 504
images
galeries, 243
impression, 509, 513–516
applications, depuis, 520
configuration avec YaST, 513
connexion, 514
CUPS, 520
dépannage
réseau, 529

fichier PPD, 515
files d'attente, 514
Firefox, 93
GIMP, 253
imprimantes GDI, 527
IrDA, 336
kprinter, 520
ligne de commande, 520
page de test, 516
pilote Ghostscript, 515
pilotes, 515
port, 514
réseau, 529
Samba, 809
xpp, 520
init, 457
ajout de scripts, 463
inittab, 457
scripts, 460–465
installation
GRUB, 473
internationalisation, 504
Internet
cinternet, 648
connexion, 646–649
DSL, 632
KInternet, 648
qinternet, 648
RNIS, 629
smpppd, 646–649
TDSL, 634
IrDA, 265, 334–337
arrêt, 335
configuration, 335
démarrage, 335
dépannage, 336

J

Java, 83
JavaScript, 83
jokers, 440

K

K3b, 151–158
CD audio, 154
CD de données, 151
configuration, 152
copie de CD, 155
KAddressbook (voir Kontact)
KAudioCreator, 134
KDE
KGpg, 107
shell, 417
kernels
caches, 500
KGpg, 107–115
approbation de clés, 111
chiffrement de fichiers, 114
chiffrement de texte, 114
chiffrement du Presse-papiers, 114
création de clés, 107
exportation de clés publiques, 109
importation de clés, 110
lancement, 108
serveurs de clés, 111
exportation de clés, 113
importation de clés, 112
signature de clés, 110
éditeur, 115
kill, 445
killall, 445
KMail (voir Kontact)
KMix, 120
KNotes (voir Kontact)
Konqueror, 79–84
appareils photo numériques, 219
démarrage, 79
enregistrement de pages Web, 81

Java, 83
JavaScript, 83
mots-clés, 81
onglets, 80
profils, 80
signets, 82
Kontact, 185–200, 268
agenda, 188, 196
assistants numériques personnels (PDA), 198
carnets d'adresses, 193
codage, 191
contacts, 187, 193
création de messages, 190
dossiers, 191
démarrage, 185
Exchange, 195, 197
filtres, 192
GroupWise, 195, 197–198
identités, 189
importation de messages, 185
listes des tâches, 187
notes, 188
pièces jointes, 191
résumé, 186
signature, 191
Kooka, 239–245
aperçus, 240–241
configuration, 243
démarrage, 239
galerie, 243–244
numérisation, 241–242
reconnaissance de caractères, 244
KOrganizer (voir Kontact)
KPilot, 201–208, 268
/dev/pilot, 203
configuration, 202
installation de programmes, 208
KAddressBook, 204
KOrganizer, 205
sauvegardes, 207
synchronisation, 206
KPowersave, 263
KsCD, 131
KSysguard, 263

L

L10N, 504
LDAP, 709–735
ACL, 716
administration d'utilisateurs, 732
administration de groupes, 732
ajout de données, 720
arborescence, 712
client LDAP de YaST , 724
configuration de serveur, 715
contrôle d'accès, 718
ldapadd, 720
ldapdelete, 724
ldapmodify, 722
ldapsearch, 723
modification de données, 722
recherche de données, 723
suppression de données, 724
YaST
modules, 726
modèles, 726
lecteurs
démontage, 443
montage, 442
lecteurs Flash, 267
lecteurs flash
amorçage depuis, 472
less, 425, 441
LFS, 559
Lightweight Directory Access Protocol (voir LDAP)
Linphone, 95
Linux

désinstallation, 490
partage de fichiers avec un autre système d'exploitation, 807
réseaux et, 605
Linux 64 bits, 411
développement de logiciels, 412
prise en charge de l'exécution, 411
spécifications du kernel, 414
ln, 437
localisation, 504
locate, 440, 499
logrotate, 497
ls, 418, 436
LVM
YaST, 62

M

masquage, 344
configuration avec SUSEfirewall2, 346
Matériel
périphériques SCSI, 61
matériel
RNIS, 629
MBR, 471–472
messagerie électronique
synchronisation, 264
mkdir, 422, 437
mobilité, 259–269
appareils photo numériques, 267
assistants personnels, 268
disques durs externes, 267
Firewire (IEEE1394), 267
ordinateurs portables, 259
sécurité des données, 266
téléphones cellulaires, 268
USB, 267
modems
câble, 632
YaST, 626
modules d'authentification enfichables PAM (Pluggable Authentication Modules) (voir PAM)
more, 425
mots de passe
modification, 447
motv, 141–144
audio, 142
dimensions, 143
programmes de lancement, 143
recherche de canaux, 142
source vidéo, 142
mount, 442
mountd, 690
MS-DOS
commandes, 427
systèmes de fichiers, 427
mtools, 427
mv, 436
mémoire
RAM, 500

N

NAT (voir masquage)
navigateurs (voir navigateurs Web)
navigateurs Web
Firefox, 85–94
Konqueror, 79–84
NetBIOS, 808
Network File System (système de fichiers réseau) (voir NFS)
Network Information Service (service d'informations réseau) (voir NIS)
NFS, 685
autorisations, 689
clients, 685
exportation, 688
importation, 686
montage, 686

serveurs, 687
nfsd, 690
NIS, 677–683
clients, 683
esclaves, 677–682
maîtres, 677–682
niveaux d'exécution, 457–460
modification, 460
modification dans YaST, 465
noeuds de périphériques
udev, 543
Noyaux
Limitations, 560
nslookup, 446
NSS, 643
bases de données, 643
numérisation
Kooka, 239–245
reconnaissance de caractères, 244–245
nxtvepg, 145
filtres, 146
importation d'une base de données, 145

O

Ogg Vorbis, 132
oggenc, 132
opd, 331
OpenLDAP (voir LDAP)
OpenOffice.org, 161–169
aide, 169
assistants, 164
Base, 168
Calc, 167
formats de document Microsoft, 162
Impress, 167
modules d'application, 161
navigateur, 166
styles, 166
sélection de texte, 165
Writer, 164–167
OpenSSH (voir SSH)
ordinateurs portables, 259–266
gestion de l'alimentation, 260, 285–297
matériel, 259
PCMCIA, 259
SCPM, 260, 273
SLP, 262
ordinateurs portatifs (voir ordinateurs portables)
OS/2
partage de fichiers, 807

P

PABX, 630
pages d'informations, 501
pages de manuel, 435, 501
pages Web
archivage, 81
PAM, 581–589
pand, 330
pare-feux, 341
filtres de paquets, 341, 345
SUSEfirewall2, 341, 346
partitions
codage, 358
table de partitions, 471
passwd, 447
PCMCIA, 259, 271
IrDA, 334–337
ping, 446
polices, 572
codées en CID, 577
TrueType, 571
X11 de base, 576
Xft, 572
portables
IrDA, 334–337
Ports

53, 666
powersave, 297
configuration, 298
processus, 445
aperçu, 445
élimination, 445
protocoles
IPv6, 612
LDAP, 709
SLP, 651
SMB, 808
protocole PTP, 218
ps, 445
Périphériques SCSI
configurer, 61
noms de fichiers, 61

Q

qaRecord, 139

R

RAID
YaST, 70
reboot, 447
RFC, 605
rm, 437
rmdir, 437
routage, 609, 639–640
masquage, 344
masques réseau, 609
routes, 639
statique, 639
RPM
sécurité, 374
rsync, 788, 801
répertoires
changement, 437
chemins, 423
création, 437
navigation, 423
structure, 418
suppression, 437
réseaux, 605
adresse de diffusion, 611
adresse réseau de base, 611
Bluetooth, 265, 326
configuration, 623–646
IPv6, 620
DHCP, 691
DNS, 621
fichiers de configuration, 638–645
hôte local, 611
IrDA, 265
masques réseau, 609
routage, 609
sans fil, 265
SLP, 651
TCP/IP, 605
WLAN, 265
YaST, 623
Résolution de noms (voir DNS)

S

Samba, 807–820
aide, 820
arrêt, 809
autorisations, 812
clients, 808–809, 818–819
configuration, 809–813
démarrage, 809
impression, 819
imprimantes, 809
installation, 809
login, 814
noms, 808
optimisation, 819
partages, 809–810
serveurs, 809–813

SMB, 808
swat, 813
sécurité, 812–813
TCP/IP, 808
SCPM, 273
changement de profil, 280
démarrage, 279
gestion de profils, 279
groupes de ressources, 279
ordinateurs portables, 260
paramètres avancés, 281
scripts
boot.udev, 547
init.d, 457, 460–465, 645
boot, 462
boot.local, 463
boot.setup, 463
halt, 463
network, 646
nfsserver, 646, 689
portmap, 646, 689
rc, 460–461, 463
sendmail, 646
xinetd, 646
ypbind, 646
ypserv, 646
irda, 335
mkinitrd, 455
modify_resolvconf, 501, 640
SuSEconfig, 466–469
désactivation, 469
sdptool, 329
secteur d'amorçage principal (voir MBR)
Serveurs de noms (voir DNS)
Service Location Protocol (SLP) (voir SLP)
shells, 417–452
Bash, 417
caractères jokers, 424
chemins, 423
commandes, 435–447
tuyaux, 425
SLP, 262, 651
enregistrement de services, 651
Konqueror, 653
navigateur, 653
slptool, 653
SMB (voir Samba)
Soft RAID (voir RAID)
son
compression de données
Grip, 133
Konqueror, 134
oggenc, 132
compression des données
KAudioCreator, 134
Ogg Vorbis, 132
enregistrement
arecord, 139
audacity, 136
qaRecord, 139
lecteurs, 125–132
amaroK, 125
GNOME, 132
KsCD, 131
XMMS, 129
mixeurs, 119
alsamixer, 121
envy24control, 123
GNOME, 120
KMix, 120
modification de fichiers, 137
puces
Audigy, 123
envy24, 123
intégrées, 122
Soundblaster Live, 123
SSH, 352–358
démon, 354
mécanismes d'authentification, 356

paires de clés, 355–356
scp, 354
sftp, 354
ssh, 353
ssh-agent, 357–358
ssh-keygen, 356
sshd, 354
X et, 357
su, 447
subversion, 787, 797
surveillance du système, 263
surveillance système
KPowersave, 263
KSysguard, 263
synchronisation des données, 264
Evolution, 268
Kontact, 268
KPilot, 268
messagerie électronique, 264
système
arrêt, 447
limiter l'utilisation des ressources, 499
localisation, 504
redémarrage, 447
système X Window (voir X)
systèmes de fichiers
ACL, 377–388
choisir, 550
codage, 358
cryptofs, 358
JFS, 555–556
LFS, 559
limitations, 559
Reiser4, 554–555
sysfs, 536
Systèmes de fichiers, 549–561
Ext2, 552
Ext3, 553–554
pris en charge, 558–559
ReiserFS, 551
termes, 549
XFS, 556–557
sécurité, 362–375
amorçage, 363–365
Apache, 779
attaques, 370–372
autorisations, 366
bogues, 367, 370
conseils et astuces, 372
DNS, 372
ingénierie, 363
mots de passe, 364–365
niveau local, 364–368
notification des problèmes, 375
pare-feux, 341
réseau, 368–372
Samba, 812
signature des RPM, 374
SSH, 352–358
système de fichiers chiffré, 266
tcpd, 375
Telnet, 352
terminaux série, 363–364
vers, 372
virus, 368
X, 369
sécurité des données, 266

T

tar, 426, 439
TCP/IP, 605
ICMP, 606
IGMP, 606
modèle en couches, 606
paquets, 607–608
TCP, 606
UDP, 606
telnet, 446
terminologie

différences avec GroupWise, 198
top, 445
TV, 141–150
téléphones cellulaires, 268
télévision
alevt, 144
EPG, 145
motv, 141–144
nxtvepg, 145
télétexte, 144
xawtv4, 147

U

udev, 543
clés, 545
jokers, 545
règles, 544
script de démarrage, 547
stockage de masse, 547
substitution, 545
sysfs, 546
udevinfo, 546
ulimit, 499
options, 499
umount, 443
updatedb, 440
USB
appareils photo numériques, 217
disques durs, 267
lecteurs Flash, 267
utilisateurs
/etc/passwd, 584, 725

V

variables
environnement, 504
Voix sur IP, 95

W

webcams
motv, 144
WHOIS, 623
Windows
partage de fichiers, 807
WLAN, 265

X

X
aide, 571
jeux de caractères, 571
optimisation, 565–571
pilotes, 570
polices, 571
polices codées en CID, 577
polices TrueType, 571
polices X11 de base, 576
SaX2, 566
SSH et, 357
systèmes de polices, 572
sécurité, 369
xf86config, 566
xft, 571
Xft, 572
écran virtuel, 569
X.Org, 565
Xen, 591
présentation, 591
Xft, 572
XKB (voir clavier, XKB)
XMMS, 129
xorg.conf
Depth, 569
Device, 568
Display, 569
Files, 566
InputDevice, 566
modeline, 567, 569

Modes, 567, 569
Monitor, 567–568
profondeur de couleurs, 569
ServerFlags, 566

Y

YaST
3D, 578
carte réseau, 623
chargeur d'amorçage
emplacement, 487
mot de passe, 489
ordre des disques, 489
type, 485
client LDAP, 724
clients NIS, 683
configuration de l'amorçage, 484
système par défaut, 488
sécurité, 489
timeout, 488
DHCP, 692
DSL, 632
gestion de l'énergie, 306
GRUB, 485
impression, 513–516
LILO, 485
LVM, 62
modem câble, 632
modems, 626
navigateur SLP, 653
niveaux d'exécution, 465
RAID, 70
RNIS, 629
Samba
clients, 818
T-DSL, 634
éditeur sysconfig, 467
YP (voir NIS)